

Staying Safe On the Internet



John Lortz - DiscoverSkills.com



discoverSkills
www.DiscoverSkills.com



Staying Safe On the Internet

*Written by John Lortz
DiscoverSkills.com*

Instructor editions
are available
for each of our computer
course offerings

Copyright © 2013
by John Lortz
11684 Meredith Ave
Omaha, NE 68164
jlortz@discoverskills.com
www.discoverskills.com
Book Revision 08112013

Who is this Guy, John Lortz?

Yes, I am a real person, and I live in the United States, Midwestern town of Omaha, Nebraska. No, my office window does not look out over a field of corn, but go about 10 blocks to the north, and you'll find one. And yes I did grow up in a small farming town... a very, very small town of 600, and loved every minute of the 18 years.

Here in Omaha, I live with my wife Sue Leavitt (another professional geek) and my son Jack (a want-to-be professional baseball player), and lead a fairly common, Midwestern life.

For 15 years, until just recently, I was Director of Education and Technology for the Senior Health Foundation (SHF), a non-profit that specialized in computer education for senior citizens. There, I developed all the class curriculum, books, and videos, as well as created and maintained the organization web sites, which included my current learning site, www.DiscoverSkills.com. I also taught most of the senior technology classes and workshops, with over 10,000 students passing through over 900 classes.

Because of the weak economy, SHF closed its doors at the end of 2010. But working for SHF was a wonderful experience, both in forming lifelong relationships with my students, and in learning how to teach and relay technical information in an understandable way. That was always the challenge, and still is today.

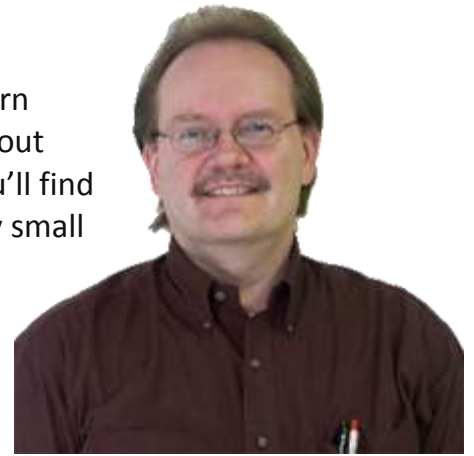
Also during my time with SHF, I assisted other retirement communities in creating senior training labs and setting up computer learning programs. I still contract and provide the learning for one of those communities, the Computer Education Center at the Landing, in Lincoln, Nebraska. This particular computer lab is state of the art, and along with my lead instructor, Wayne Casper, we provide over 40 different class offerings from the very basic for those just getting started, to the more advanced for those who want to learn eBay, Facebook, Photoshop editing, or PC maintenance.

Besides teaching at SHF, I continue to be an adjunct instructor at the College of St. Mary here in Omaha. I've been teaching computer-science related classes there since 1988, including web page design, database management, various programming and digital imaging classes, and advanced business applications. Teaching at the college level has been a great balance to teaching seniors technology, and by blending the methods used for each group, I think I've come up with some great insights on technology learning.

On the writing side, I served as a freelance writer for *Smart Computing*, *PC Today* and *CPU* magazines, where I published more than 30 articles on computer related topics.

As for some odds and ends, I served on the Omaha Public Schools Internet Advisory Committee, and currently act as a volunteer video media advisor to Skinner Magnet School. I was a featured speaker at the Nebraska AGPAM Conference, and I've presented at the national AAHSA Annual Meeting. In addition, I was a keynote speaker at the Nebraska Society for Healthcare Marketing and Public Relations conference, presenting ideas on Internet marketing and Web page design.

I have a Master's degree in Computers in Education, but to be honest, most of my initial technical, geeky experience came from the five years I acted as the Director of Information



Systems for a small software development company here in Omaha. And following that job, I did computer and network consulting for a few years, before ending up at SHF.

Whew... Ok, so I've talked a bunch about myself. The thing is, I've been blessed with lots of great experiences working with technology and students who are interested in technology. Although I never set out to be one, I guess you could say I've become a professional technology educator. But along the way, I've also become a PC geek, networking geek, web-video specialist, web site designer, and a bunch of other nerdy things that just went with the territory that my life traveled through.

So, that's it. That's me. That's who I am and where I've been. Oh, and hopefully, I'm not done yet! Feel free to explore our sites and take in what we offer there. I also invite you to visit our main learning portal, DiscoverSkills (www.DiscoverSkills.com). And if you have any questions, feel free to shoot them my way.

I'll even listen to YOUR life story, if you want to tell me!



DiscoverSkills

A handwritten signature in black ink, which appears to be "John Lortz".

www.DiscoverSkills.com

DiscoverSkills.com is a technology learning portal created by John Lortz to assist students of all ages in understanding and using computer, photography, and mobile device technology. We do this through eBooks, video courses, and webinars.

For more information, email us at jlortz@discoverskills.com or visit one of our Web sites.

DiscoverSkills (our main site) – www.discoverskills.com

Our YouTube Channel – www.youtube.com/discoverskills

Discover Computer Basics – www.discovercomputerbasics.com

Discover File Organization – www.discoverfileorganization.com

Discover Internet Safety – www.discoverinternetsafety.com

Discover iPads & iPhones – www.discoveripads.com

Discover Windows 8 – www.discoverwindows8.net

Discover Facebook – www.discoverfacebook.net

Discover Photo Story – www.photostoryskills.com

Table of Contents

Introduction – page 1

Understanding How the Internet Works – page 1

The Physical Connection (Communication Lines and Hardware)	1
The Software that Makes the Hardware Connection Work	3
The Internet Protocol	4
Addresses on the Internet	4
The Ports on Your Computer	6
Internet Packets	7
Putting it All Together-A practical example	8

How You Are Vulnerable – THE BIG PICTURE – page 11

An Important Fact to Always Remember – page 13

Hackers	13
Who Are They?	13
How Are You Vulnerable?	14
How To Protect Yourself	16
Make Sure Your Firewall is ON	16
An alternative to a Firewall - Routers	18
Keep software updated with the latest patches	19
Create Strong Passwords	20
Phishing Emails	21
Dictionary crack	21
Brute Force	21
Weak Passwords	22
Strong Passwords	22
How do I remember all those passwords?	23

Viruses 24

Program Viruses	24
Macro Viruses	24
Worms	24
Trojan Horses	25
How they infect	25
Virus symptoms	25
Who Creates Viruses?	26

Protecting Yourself Against Viruses	27
Use an Anti-Virus Program	27
Keep the Anti-Virus Program Up-to-Date	29
Let Your Browser Help You Out	29
Be Cautious of E-Mail Attachments	30
Download from Reputable Sites	31
Keep a Backup of Your Important Data	31
What If You Get a Virus?	31

Spyware and Malware 33

Adware	33
Malware	34
Where Does Spyware Come From?	35
How Does Spyware Infect Your Computer?	35
What Do You See with Spyware and Malware?	36
Getting Rid of the Problem and Protecting Yourself	36

Keeping Private Information Private! – page 39

Online Transactions and Personal Information	39
SSL Certificates	40
Know Your Merchant	41
Browser Cookies	41
Secure E-Mail	43

Anonymous Browsing	44
ActiveX Controls and Java Applets	45
Facebook Privacy	46

Where Do I Go from Here? – page 48

An Internet Safety Checklist – page 49

Appendix A: Resources to Help You Become More Secure – page 50

Appendix B: A WiFi (Wireless Networking) Primer – page 51

Disclaimer and Terms of Use Agreement – page 56

Introduction

Without a doubt, the Internet is vast and fascinating place that provides information and resources on every imaginable topic and lets you quickly and easily communicate with family and friends. For many, it's hard to imagine life without the Internet. But as you come to understand the more you use it, the **Internet does have a dark side**. Yes, there are undesirable places you probably don't want to visit, but the dark side we're referring to here come in the form of outside **intrusion, loss of privacy**, and just plain nuisances we could certainly do without.



In this book I'll help you understand the threats you encounter on the Internet, where they might come from, and what you can do to protect your computer from them. Along the way, you'll also learn a bit more about how the Internet works, so that you can fully understand why protecting yourself is important.

Understanding How the Internet Works

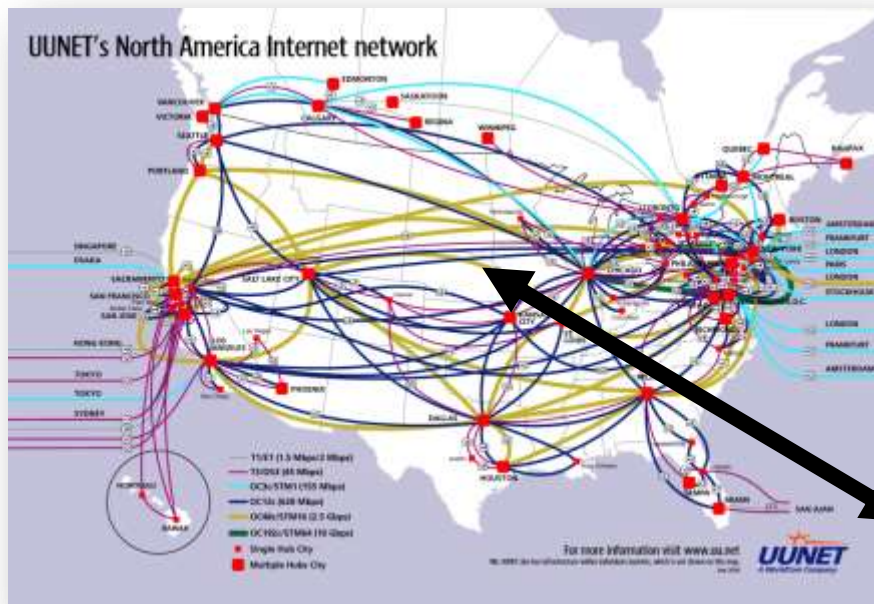
When you log your computer (or tablet, or smartphone) onto the Internet, it suddenly becomes connected to a vast web of interconnected computers that span the world.

To help you understand how your computer is vulnerable to attack while on this web, there are some basic facts you must first learn about your Internet Connection and how the Internet works.

The Physical Connection (Communication lines and hardware)

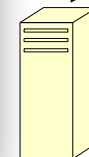
The Internet has a **Backbone** that consists of high-speed communication channels running across the country and around the world. The backbone is operated by private companies such as AT&T, Century Link, ComCast, Cox, and others, and consists of underground lines, microwave transmissions, and satellites. In reality, the Internet backbone is setup just like the backbone of our telephone system. But unlike the phone system, it only transmits our Internet data.

Let's start with the BIG picture and work our way down...



This is NOT a good representation of the Internet backbone, since the Internet is really a **world-wide** system.

NODE
(Your Computer)



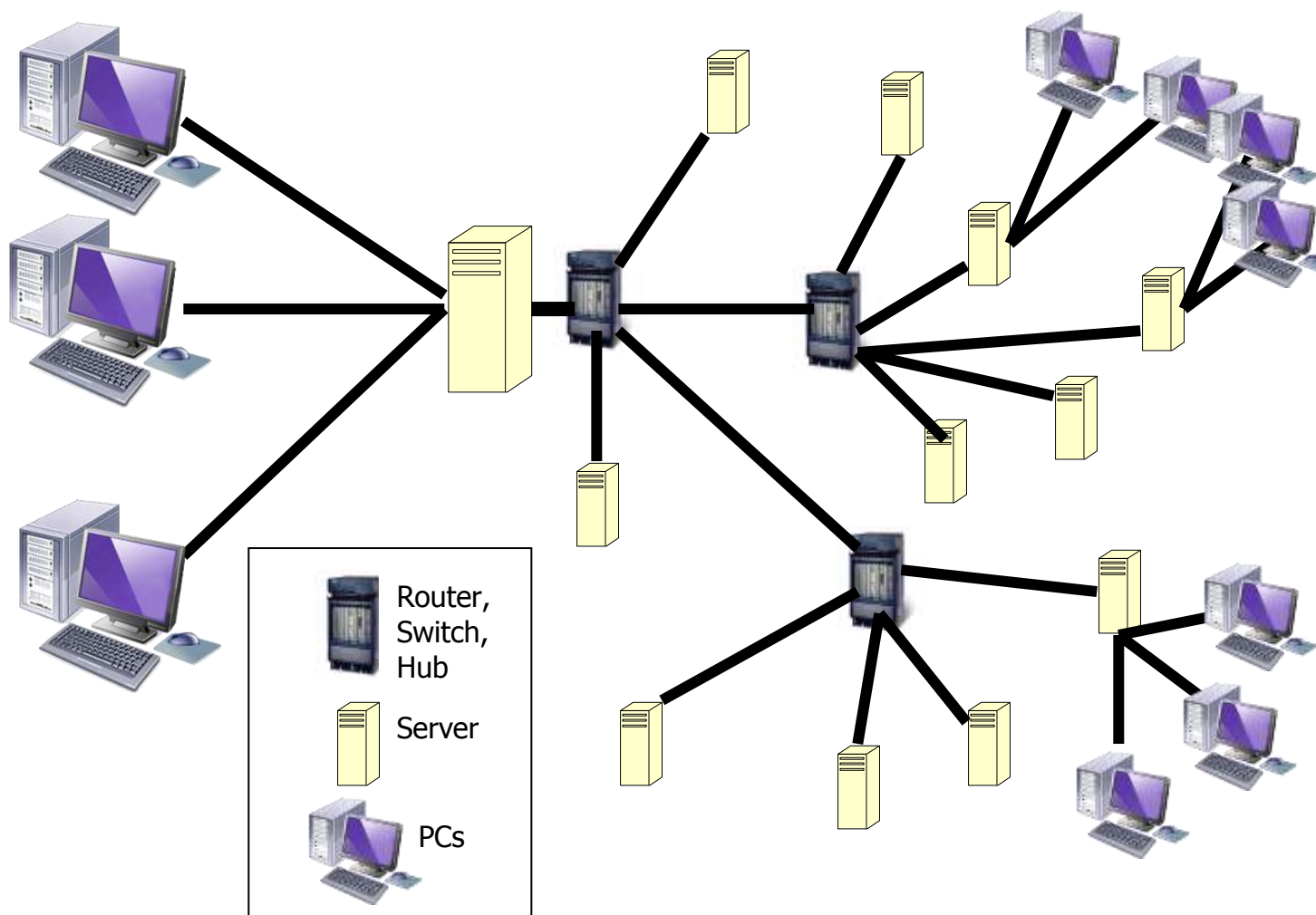
Point of Presence
(Your ISP)

Where different Backbone channels meet, you have an Internet Exchange Point, or **Network Access Point (NAP)**. Some of these points are also called Metropolitan Area Exchanges (**MAE**). These points are owned and managed by private companies such as MCI WorldCom and Ameritech, and are what allows the various communication companies to share lines so that the network can cover the entire country and globe.

Individuals connect their computers to the Internet at **Points of Presence (PoPs)** which are maintained by **Internet Service Providers (ISP)**. We often call the individual computers, **nodes**.

Hardware and software devices such as **hubs**, **switches**, and **routers** are at the connecting points of all the various Internet communication lines. They allow a smooth and organized flow of information between all the smaller networks of computers on the Internet.

Companies such as **Cisco** and **Level 3** make the hardware devices that connect all the Internet components together.



When you connect to the Internet, your computer becomes part of this vast network. However, unlike the computers that actually make up the Internet (called **servers** or **hosts**), your computer can NOT be accessed by others who are connected. In this way, **your connection is really a one-way street** where you can go out to the servers and get information, but nothing can come back to your computer unless you ask for it. ***At least, this is the way it's SUPPOSE to work.***

The Software that Makes the Hardware Connection Work

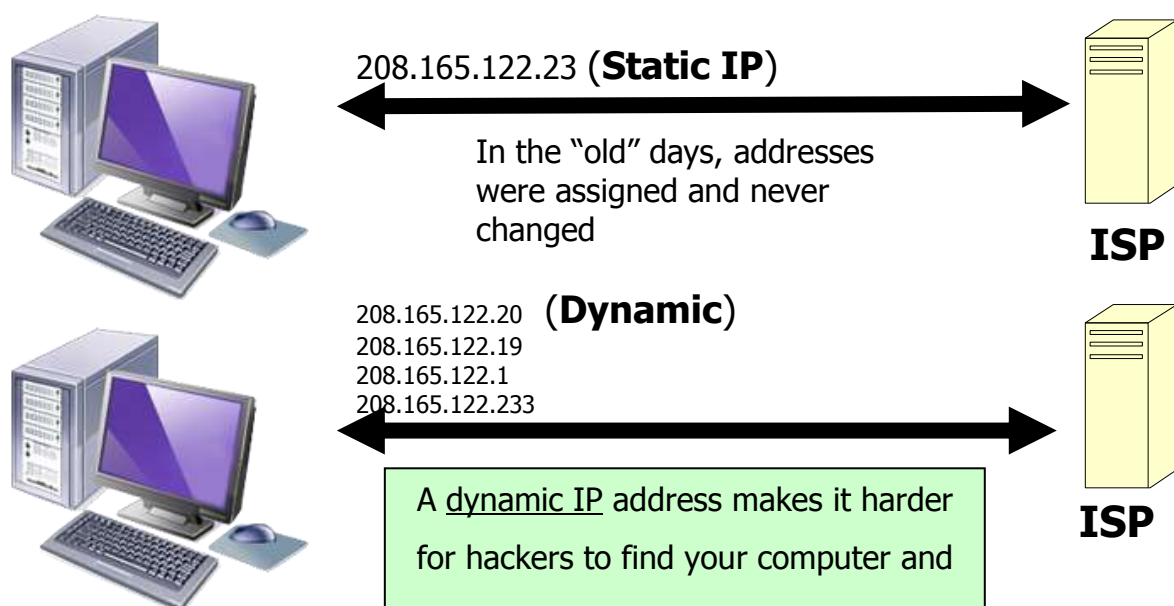
Now that you've seen how all these computers are connected physically, let's talk about what really makes the connection work. As part of Microsoft Windows on your computer, and as part of the operating system on the Internet servers, there is special **software that let's one computer talk to another**. We sometimes refer to these programs as "**protocols**", which simply means they are ***rules that each computer must follow so they can communicate with each other.***

The Internet Protocol - The main protocol of the Internet is called **TCP / IP** (Transmission Control Protocol / Internet Protocol). TCP/IP is really two protocols that work together to let Internet communication take place.

Addresses on the Internet - So that all the computers on the Internet can communicate with each other, each computer that is connected to the Internet has an **IP Address**, which is a series of numbers that looks like this: **208.164.129.115**

Your computer's IP address is **assigned by your Internet provider**, who has a large block of addresses it can give out. Most Internet providers assign your address **dynamically**, meaning that it's automatically assigned each time you connect through a dial-up connection, or for broadband (cable and DSL), assigned and re-assigned at various times throughout the day or week.

A big reason that your provider assigns addresses dynamically (which also means you get a different address each time one is assigned), is **for your protection**. With a constantly changing address, there is a reduced chance for Internet intruders to find your computer and attempt to access it.



To See Your IP Address:

In *Windows XP* Choose Start / Run, type in **command**, and click OK. In *Windows 7* type "command" at the Start / search box and then choose Command Prompt.

This opens a command window. At the flashing prompt, type **IPCONFIG** (for Windows XP, 7) or **WINIPCFG** (for Windows 98/ME) and press ENTER. You should see your current IP address displayed.

To See a Sites Address:

At the same prompt, type **ping www.yahoo.com** and press ENTER. This causes your computer to send out 4 short signals to Yahoo, which should answer. If you get no answer, your are not connected to the Internet. Pinging is a way to test Internet connections, or test to see if an Internet server is up and running. Also notice that Yahoo has an IP address, just like all other computers on the Internet. When you are finished, type **exit** and press ENTER.

208.165.122.20



```

C:\Users\jlortz>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . : Lortz_Network
    Link-local IPv6 Address . . . . . : fe80::9994:a3f9:3ad4:e2da%10
    IPv4 Address. . . . . : 192.168.2.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
Tunnel adapter isatap.Lortz_Network:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : Lortz_Network
Tunnel adapter Local Area Connection* 37:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:9d38:6ab8:20dc:496:bbf2:d372
    Link-local IPv6 Address . . . . . : fe80::20dc:496:bbf2:d372%44
    Default Gateway . . . . . : 

C:\Users\jlortz>
```

```

C:\Users\jlortz>ping www.yahoo.com

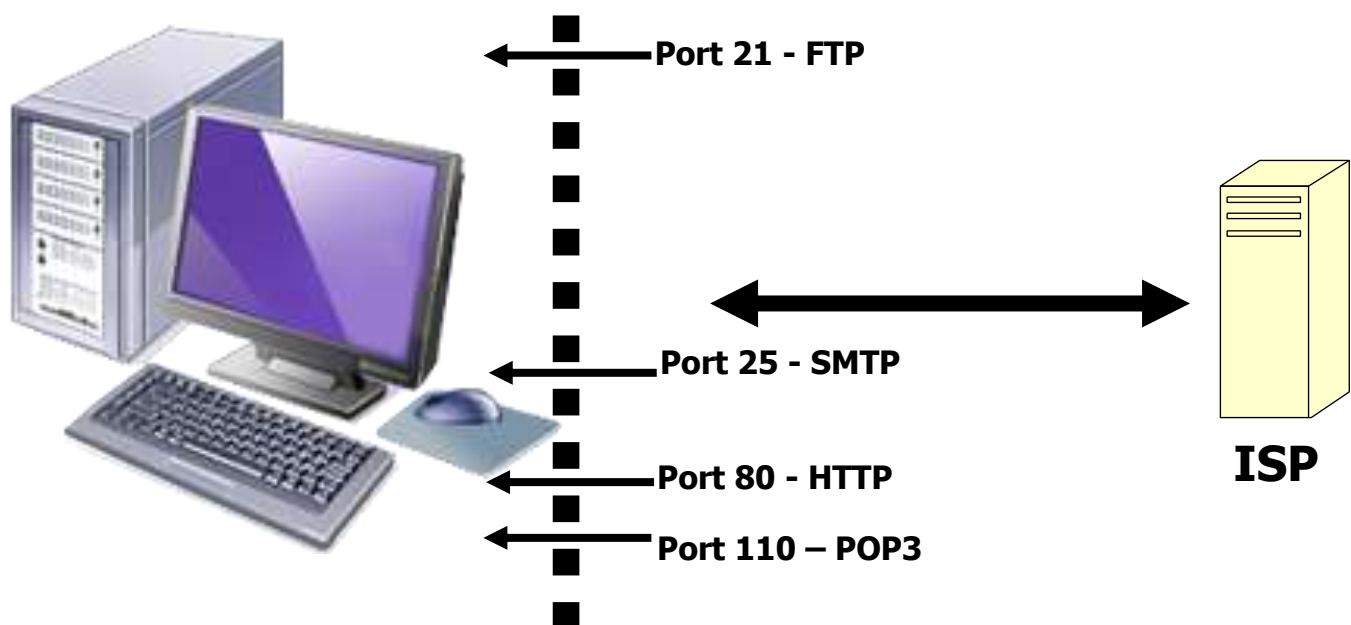
Pinging ds-any-fp3-real.wa1.b.yahoo.com [98.139.180.149] with 32 bytes of data:
Reply from 98.139.180.149: bytes=32 time=187ms TTL=51
Reply from 98.139.180.149: bytes=32 time=74ms TTL=51
Reply from 98.139.180.149: bytes=32 time=106ms TTL=51
Reply from 98.139.180.149: bytes=32 time=154ms TTL=51

Ping statistics for 98.139.180.149:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 74ms, Maximum = 187ms, Average = 130ms

C:\Users\jlortz>
```

The Ports on Your Computer – In addition to TCP / IP and your IP address, there's one more software component we need to discuss with regards to your Internet connection. Each time you connect to the Internet and perform a specific task, such as browse to a Web page, send an E-mail, or download a file, your communication with the Internet takes place through one of thousands of different **ports**, which are assigned a number from 1 to 65535.

The ports we are referring to here are NOT the plugs on the back of your computer (although these also are called ports), instead, these ports are **small communication openings** in the Windows software that let signals pass back and forth. Each port has a very specific type of communication it lets through and no other. For example, **port 21** is only used for download files (File Transfer Protocol), **port 25** is only used for sending e-mail (Simple Mail Transfer Protocol), and **port 80** is used for Web pages (HyperText Transfer Protocol).

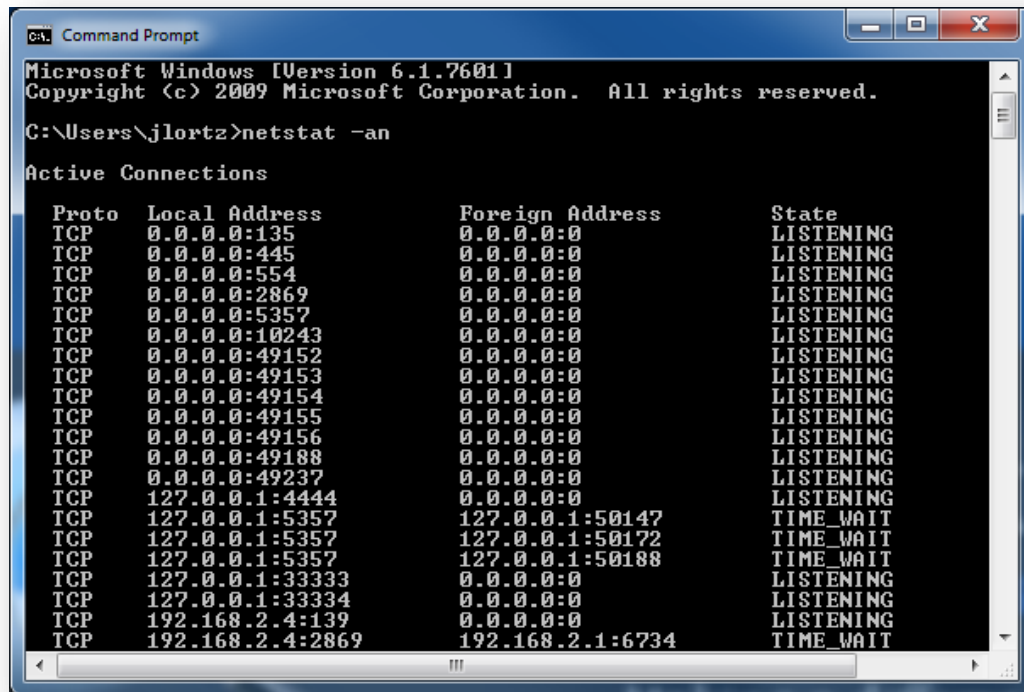


There are lots of places you can visit on the Internet, to see a list of the common port numbers and what they are for. I suggest you visit www.wikipedia.org and in the search box type **tcp port numbers**.

On the next page we have an exercise where you can see some of the ports you have open on your computer.

Try This: Go back to the command prompt window you opened on the previous exercise. At the flashing prompt, type **netstat -an**. You should see a list of TCP ports that are open and listening for communications.

In the screenshot below, the TCP port number is preceded by a colon and follows an IP number. For example, 192.168.2.4:**139** (139 is the port number here)



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\jlortz>netstat -an

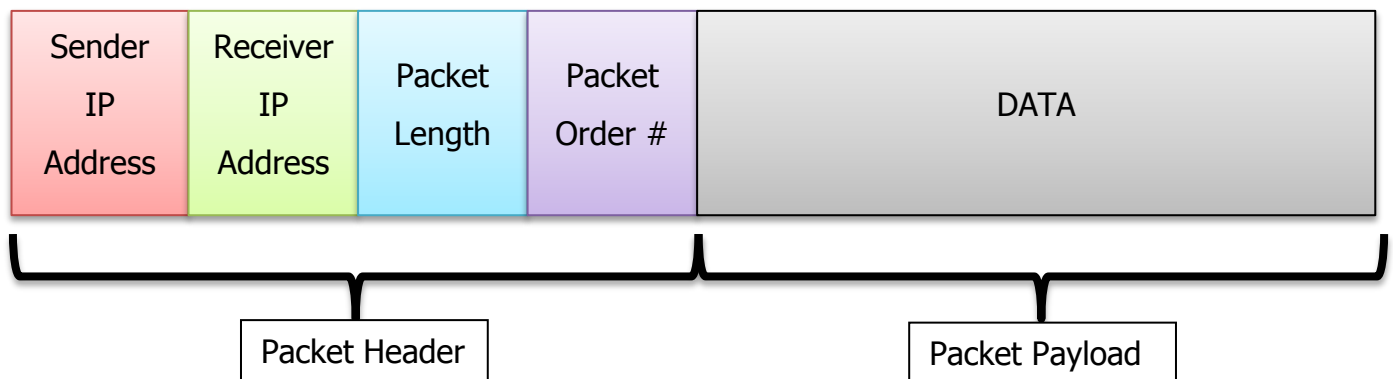
Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135               0.0.0.0:0               LISTENING
TCP    0.0.0.0:445               0.0.0.0:0               LISTENING
TCP    0.0.0.0:554               0.0.0.0:0               LISTENING
TCP    0.0.0.0:2869              0.0.0.0:0               LISTENING
TCP    0.0.0.0:5357              0.0.0.0:0               LISTENING
TCP    0.0.0.0:10243             0.0.0.0:0               LISTENING
TCP    0.0.0.0:49152             0.0.0.0:0               LISTENING
TCP    0.0.0.0:49153             0.0.0.0:0               LISTENING
TCP    0.0.0.0:49154             0.0.0.0:0               LISTENING
TCP    0.0.0.0:49155             0.0.0.0:0               LISTENING
TCP    0.0.0.0:49156             0.0.0.0:0               LISTENING
TCP    0.0.0.0:49188             0.0.0.0:0               LISTENING
TCP    0.0.0.0:49237             0.0.0.0:0               LISTENING
TCP    127.0.0.1:4444            0.0.0.0:0               LISTENING
TCP    127.0.0.1:5357            127.0.0.1:50147         TIME_WAIT
TCP    127.0.0.1:5357            127.0.0.1:50172         TIME_WAIT
TCP    127.0.0.1:5357            127.0.0.1:50188         TIME_WAIT
TCP    127.0.0.1:33333           0.0.0.0:0               LISTENING
TCP    127.0.0.1:33334           0.0.0.0:0               LISTENING
TCP    192.168.2.4:139           0.0.0.0:0               LISTENING
TCP    192.168.2.4:2869         192.168.2.1:6734        TIME_WAIT
```

Internet Packets – The final part of the software equation, I think is probably the most amazing. Whenever your computer communicates through ports to the Internet using the TCP / IP protocols, the message you send and the message you receive is sent in the form of **packets**.

Think of it this way. The information that is sent back and forth is first **chopped into small pieces** (packets) which are **independently sent** across the Internet. Each piece has its own delivery information which helps it to where it's going.

Here is a diagram that illustrates what a **single packet might look like** (and please note, that in my attempt to keep this simple, this is NOT an accurate representation of a packet).



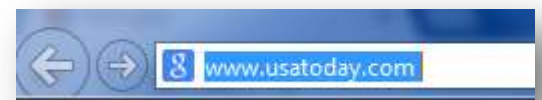
Putting it All Together: A Practical Example

Ok, so we've seen how the Internet is physically connected (the hardware part) and now we've covered how the software makes it all work.

Lots of geeky stuff, to be sure!

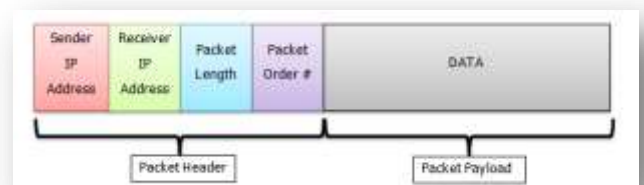
So how about we pull this all together into a practical example of **what happens when you're browsing on the Internet**.

Let's say you start a browser like **Internet Explorer**, and type in www.usatoday.com to visit USA Today's web site. When you hit ENTER, this happens...

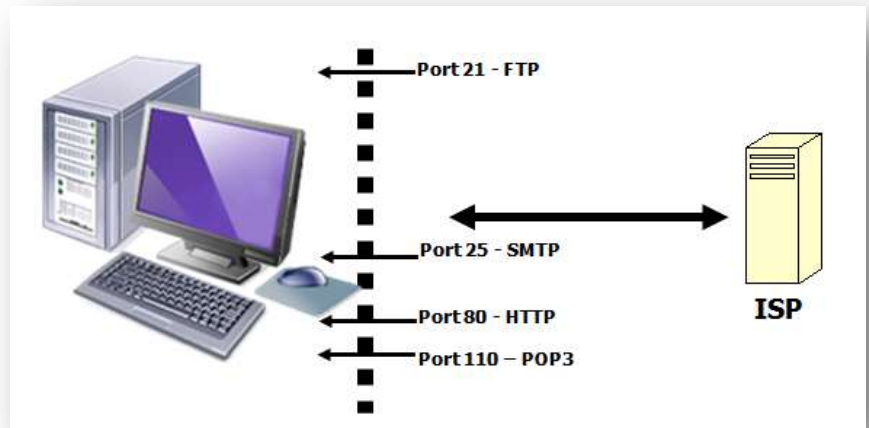


1. Your message (a request for a web page) is chopped into small pieces (**packets**) by the **TCP/IP protocol** that is part of the Windows operating system.

Each packet contains a **header** that includes such information as your IP address, the recipients IP address, and the packet order number. It also includes the **payload** (a message chunk).

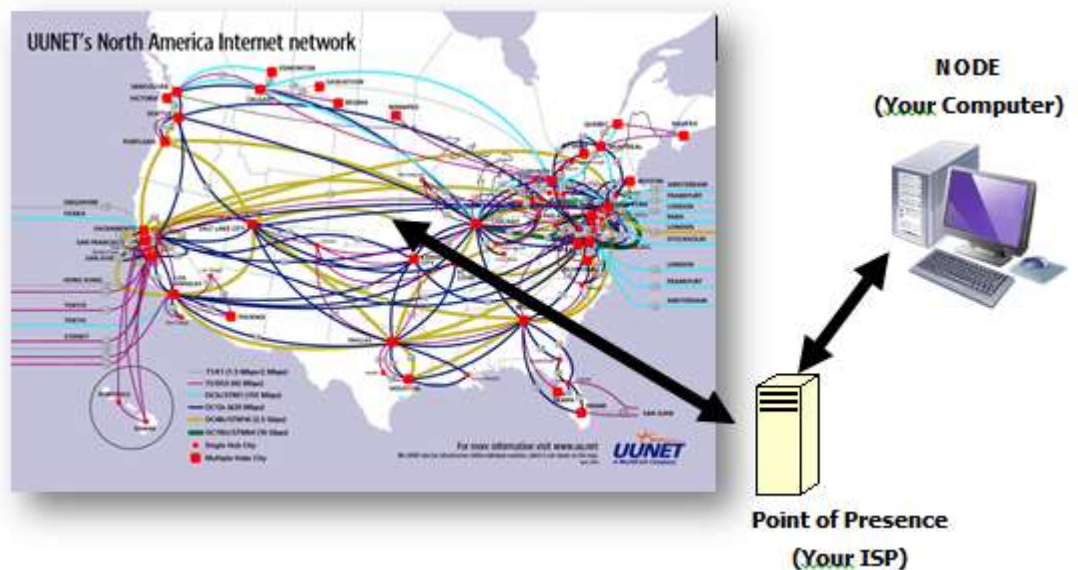


2. The packets are **transmitted** to your ISP (Internet Service Provider, or point of presence), out from your computer through **port 80** (the HTTP or Web port).

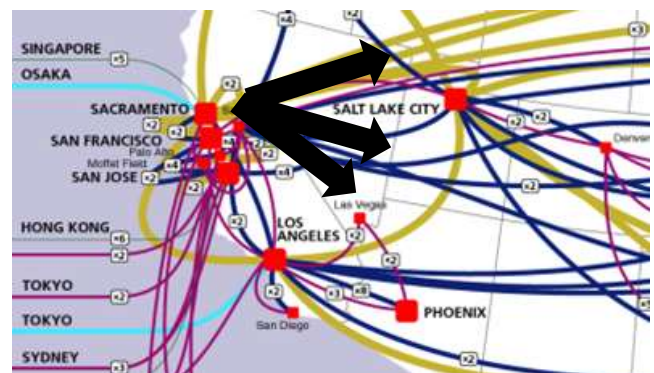


3. The ISP **recombines** the packets and checks to make sure there were no errors.

The ISP then determines where the message needs to go, and again breaks it into **packets** and sends it out to the **Internet Backbone** to the destination.



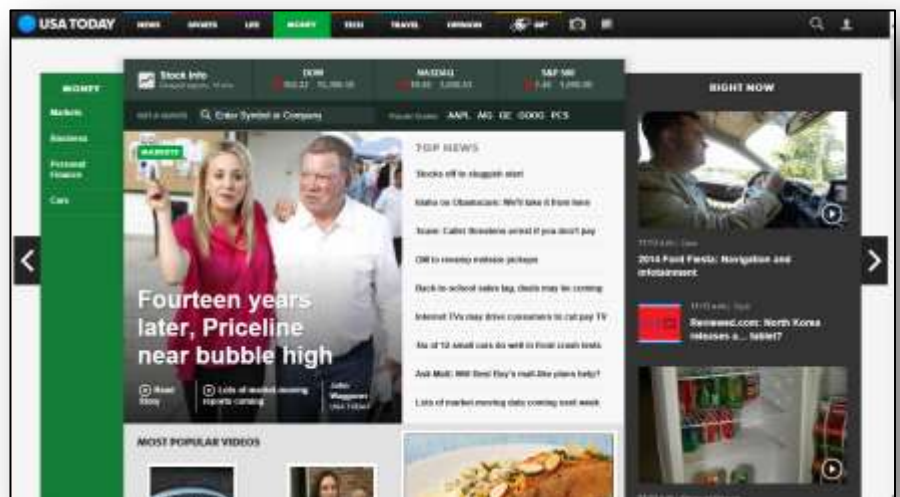
4. During the journey, the packets can travel **separate pathways**, and jump from **router** to router until the destination is reached. One purpose of the router is to find the best pathway for a packet at any given microsecond.



5. At the destination (in this case, USA Today's server), the packets are **recombined** into the request or message.



6. When USA Today **sends you back the Web page**, the exact same thing happens the other direction.



The amazing thing is... this entire process happens EVERY TIME you get information from the Internet. And it happens in a matter of SECONDS! Mind boggling, to be sure!

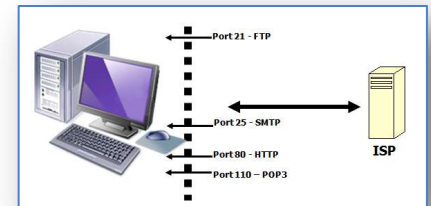
But now let's look at how the way the Internet works, also makes you **VULNERABLE!**

How You Are Vulnerable – the BIG PICTURE!

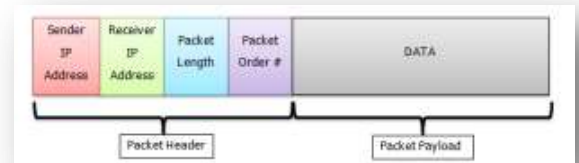
At every point in the communication path I walked through in the previous section, security measures have been put in place by Windows. However, even the best laid plans can be exploited by someone who has the skill and the motivation.

Here are a few examples of how **Internet threats** can take advantage of the technology behind the Internet:

- Because of certain **Windows security flaws**, certain **ports** can potentially be used by outside individuals to access your computer and take advantage of it.



- As **packets** travel on the Internet, they are not normally encrypted, so they can be **intercepted** and **read** by those with the right know-how.



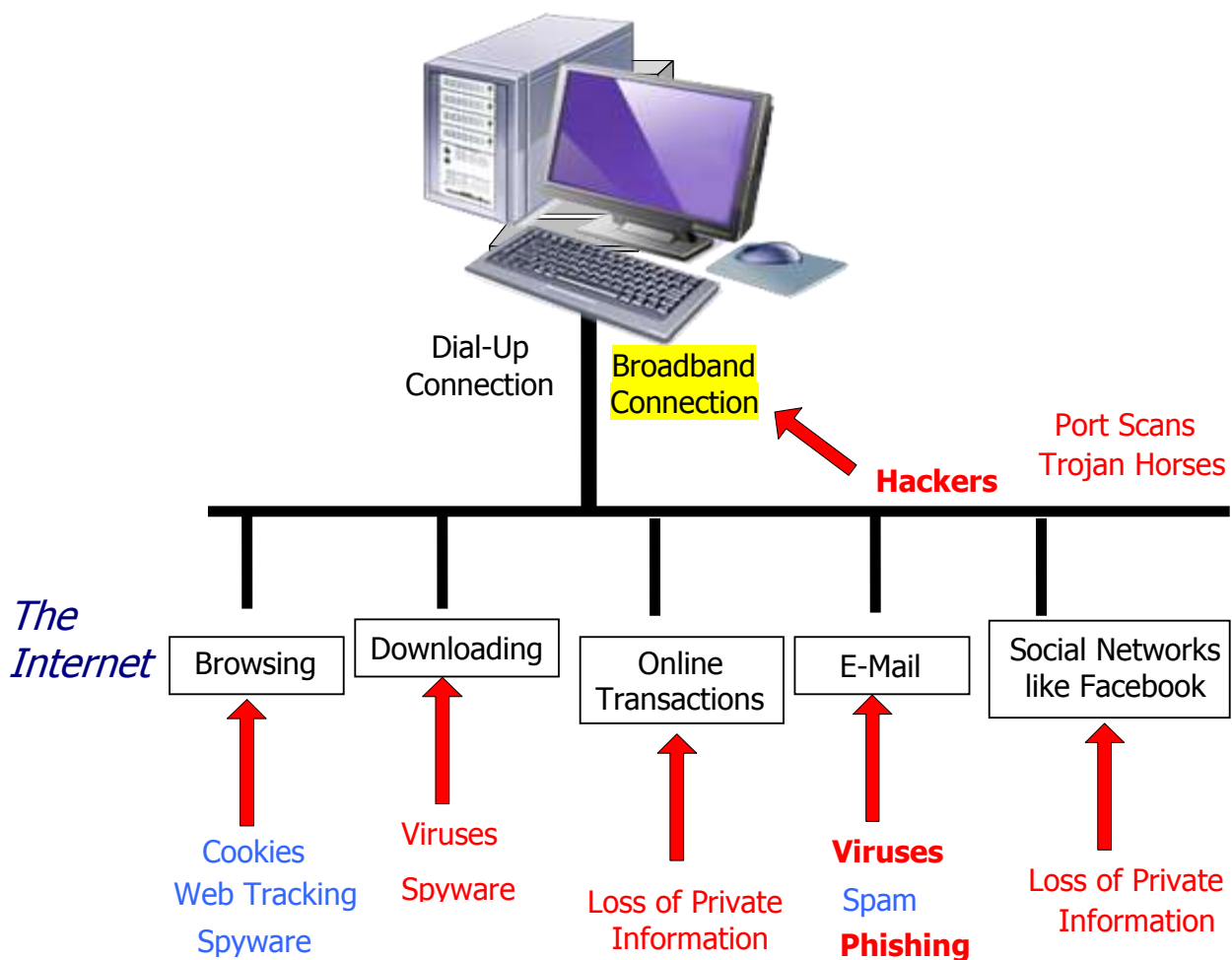
- Since your computer has an **IP address** that is used to identify it on the Internet, someone on the Internet can find that address and potentially exploit your computer.

208.165.122.20



And the list goes on. The point is, whenever your computer is connected to the Internet (which it is the entire time it's turned on), there are threats that take advantage of holes in the technology, and attempt to access and use your computer and private information in harmful ways.

The illustration on the next page illustrates the most important of these threats, and over what part of the Internet they typically attack you.



Although we'll discuss each in detail next, here's a brief summary:

- **Hackers** (crackers) search for your IP address, scan your ports, and then sneak Trojan horse, keyloggers, and virus programs onto your computer, opening even bigger access holes in your connection that they can take advantage of.
- **Viruses** infect your computer often via E-mail attachments, where they replicate and spread to other computers.
- In a **non-secure online transaction**, the information you type, such as a credit card number, can be intercepted and stolen.
- **Phishing Emails** try to lure you into clicking and visiting a fake site that has you type in your username and password so that they can be stolen.
- You can lose personal information by not correctly securing it on **social network sites** like Facebook and Linked-In.
- **Downloads** can contain viruses and spyware programs.
- As you browse the Internet, you can unknowingly pickup advertising and tracking **cookies**, as well as **spyware programs**.

Of all these threats, **hackers**, **viruses**, **spyware**, and **phishing emails** are probably the most common and most likely to be a threat. In the next section we will start with those, and then later in the book cover the other threats.

AN IMPORTANT FACT to always remember!

Always keep in mind that regardless of how you protect yourself, **you can never be totally secure on the Internet**. As faithfully as you might do the various things I am going to suggest, there's still chance your computer will someday be compromised by an Internet threat. The only sure way of total protection, is to NOT be connected to the Internet (and who wants to do that?).

However, there are some very practical things you can do to minimize those threats, almost to the point where you no longer have to worry (at least quite as much).

I start giving you that information in the next section.

Hackers

As defined by the popular press, a **Hacker** is someone who breaks into computer systems for illegal or unethical reasons. In the computer world, the term used to refer to an individual who possesses high technical skills and constantly experimented with programs and hardware to learn how they worked.

Perhaps the term **cracker**, is a better label someone who breaks into computers. However, we'll use the word hacker, since it's the term most people are used to hearing.

Although some hackers break onto machines for the sake of profit or gain, many try to hack Internet computers just for fun, or to brag about their technical prowess to their hacker friends.

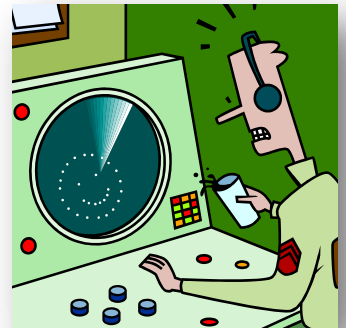


How are you vulnerable? – In the last section you learned about **IP addresses** and **ports**. Now it's time to see how a hacker uses those Internet features to illegally access your computer. To help you understand, let's run through a typical hack.

- A hacker will first run a program called a “**sniffer**” that scans a range of IP addresses, looking for those that are active. Basically, a sniffer **pings** the addresses to see if they are there. If a computer responds, it's a “live one” and its IP address is stored in a database.



- Now that the hacker has a database of active IP numbers, they run a program called a “**port scanner**” on each IP address to look for possible open ports that can be exploited.



If a hacker, using port scanning software, finds an IP address with an open port, they can use that small opening to upload a **virus** or **Trojan horse**, to that computer.

Using the Trojan horse, a hacker can **take complete control** of the computer, access private information, capture and retrieve all of your keystrokes (and therefore your passwords), or even launch attacks on other computers across the Internet, which is one of the most common reasons home computers are hacked.



Hackers can also attempt to get your **account passwords** so that they can access your accounts and get at private information, or even use your accounts for some other illegal purpose.

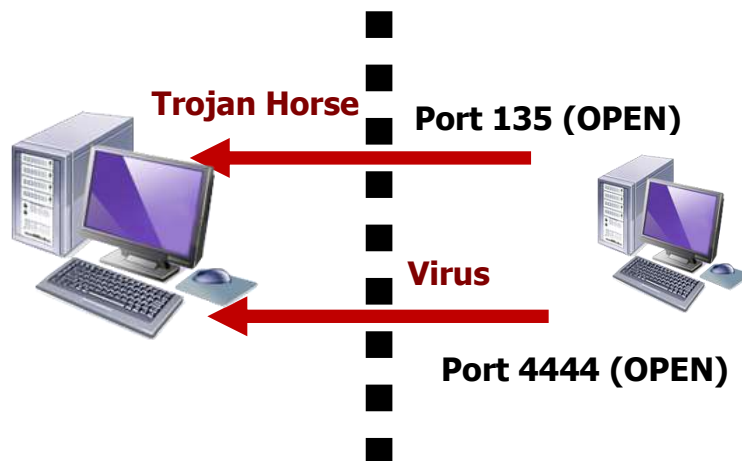
Does what I just described happen in the real world? Yes, every day! Let's take our example a step farther, and relate a type of invasion that really happened some years back.

The Blaster Virus (Win32/MSBlast)

A hacker writes a program (called **Blaster**) that automatically **scans IP addresses** looking for an open **port 135**.

When it finds one, it sends an exploit command to that port, and when communication is established, it sends a worm virus through **port 4444**.

The worm infects the machine, replicates, and attempts to spread using the same technique. It also changes the Internet Explorer Home page (**browser hijack**), opens a back door for the hacker through other ports, sending the IP address and port number to a remote computer, and finally, sets up a timer for a DoS (**Denial of Service attack**) where the infection machine begins repeatedly pinging a host computer on a certain day and time.



More about DoS Attacks

One of the most common ways for a hacker to bring down an important web site, such as PayPal, Amazon, or the New York Times is by using a DoS (denial of service) attack. A hacker writes a worm to infect thousands of computers with a payload that goes off at the same time on all the machines. That payload tells the computer to repeatedly "ping" the target web site, which effectively brings it crashing down.

How to Protect Yourself from Hackers – There are multiple steps you can take to help prevent hacker attacks.

1. Make Sure Your Firewall is ON.

Here is what a “firewall” does on a PC:

Act as a barrier between your computer and the Internet, **preventing your computer ports from responding** to sniffer requests.

Monitor all incoming and outgoing packets, blocking those that are not authorized (packet filtering). This not only protects you from a hacker sending unwanted files, but also prevents your computer from secretly sending out information you don’t want to leave.



The most common type of home computer firewall is the **software firewall**, and the GOOD NEWS is that If you have Windows XP, Vista, or Windows 7 or 8, you have a **free firewall** built into the program called **Internet Connection Firewall** (ICF) or simply **Windows Firewall**.

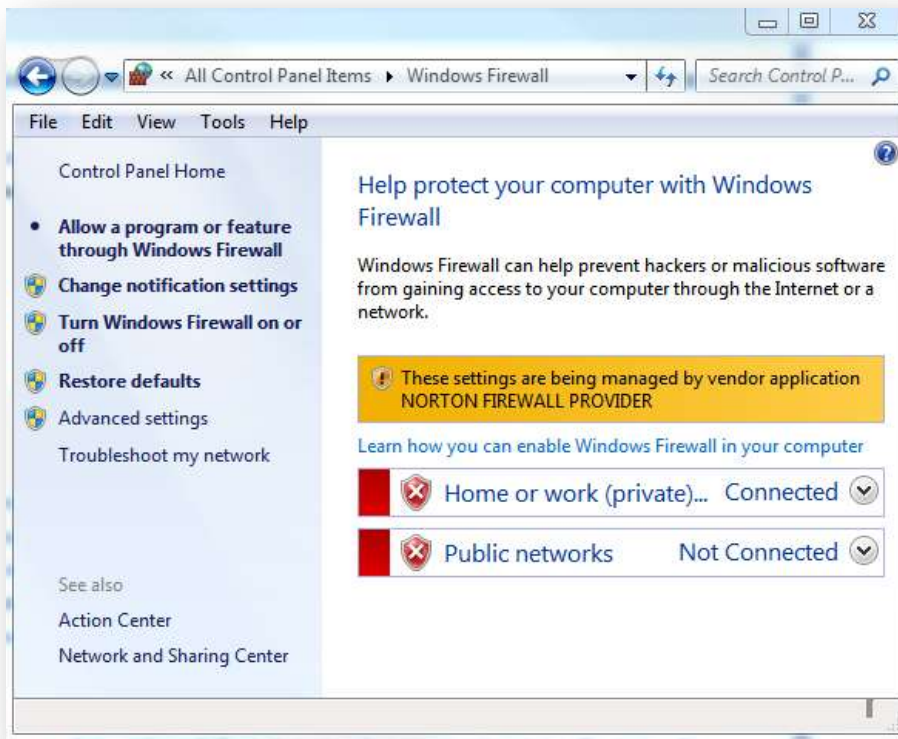


Windows Firewall is **automatically turned on** when you first setup Windows. *But To check the Windows Firewall and make sure it’s on, go to the **Control Panel**, and start the program called Windows Firewall.*

On the right is how it looks in older versions of Windows. Notice it is a simple ON and OFF type of system. For your best protection, you should have it set to ON.



Here's how it looks in **Windows 7 and 8**.



Note that in this screen shot, the computer we're using has Norton 360 installed, and THAT firewall is turned on instead of the Windows Firewall.

NOTE: Since software firewalls interfere with each other, you should **only have ONE installed at a time**. This is also true for Anti-virus programs, which we discuss in the next section. Many of the "**Internet security packages**" you purchase at the store include their own firewall that automatically disables the Windows firewall, as Norton has done in my example here.

And speaking of Norton 360, besides the free firewall you get with Windows, there are LOTS of **internet security products that include firewall protection** that is often more robust than what Windows offers. Here are some companies that offer those firewalls

Zone Alarm Free Firewall (free) at www.zonelabs.com

Outpost Firewall (free) at free.agnitum.com

Norton Internet Security (or 360) at www.symantec.com

McAfee Total Protection at www.mcafee.com

To find the latest reviews on these products and many others, I suggest you visit CNet (www.cnet.com) or PC World (www.pcworld.com) and search for "internet security".

As an alternative to a software firewall, you can use a **router** as a firewall. Routers can be purchased at the local computer store, and are primarily used at home to connect more than one computer to the Internet. However, they also act like a firewall by shielding the IP address of your computer from outside view by using a technology called **NAT** (Network Address Translation). Here's how it works:

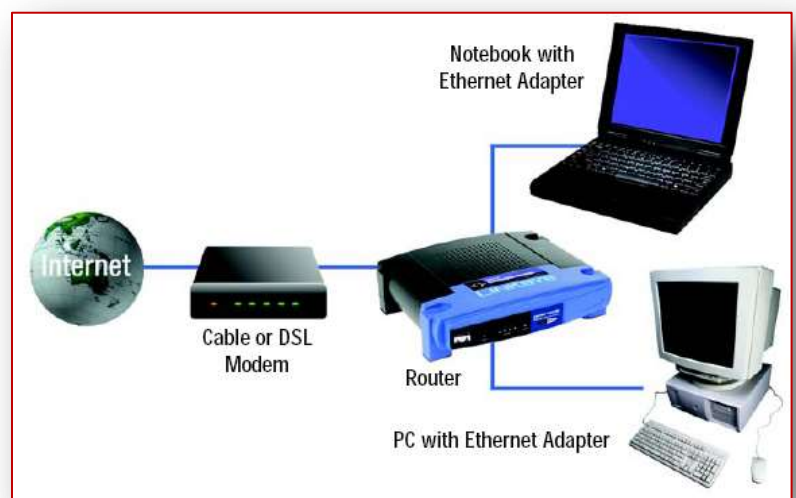
You connect your router to your cable or DSL modem, and connect your computer(s) to the router.

Your ISP assigned IP number is given to the router.

Your router assigns new, "private" IP numbers to your computer(s).

The outside world can't see the private IP numbers, and therefore, can't see your computer(s) to hack onto them.

For additional cost, you can buy a true "**Firewall**" **router** that works like a regular router, but also includes built-in firewall software that actually looks at all the incoming and outgoing packets, making sure there's nothing harmful in them. And all of what we've mentioned here is also the same for "wireless routers" which let you connect to the internet at home without any cables.



Technical Note: Many home users are now installing "**wireless**" **networks** using Wireless routers. Everything we've discussed here also applies to wireless routers; however, with wireless networking there are additional security concerns. If you go wireless, make sure you read your user manual for security settings and especially pay attention to **WEP** or better yet, **WPA** (which are both wireless encryption methods), change your **SSID** (network identification name) to some other name than the default, and change the **administrative password** to something other than the default (factory) setting.

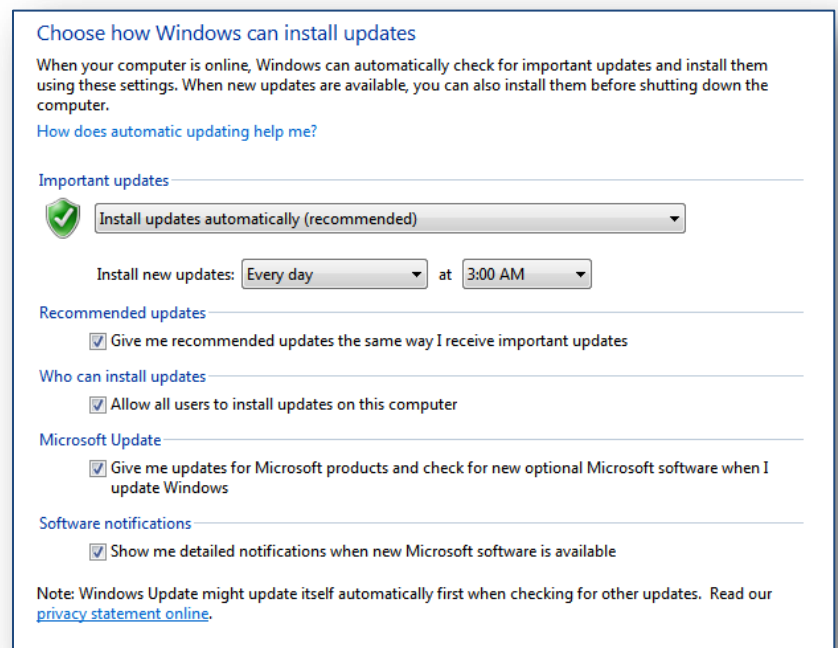
In an Appendix at the end of this book, I talk more about Wireless Networking.

2. Keep your software updated with the latest patches – Besides using a firewall, this is one of the most important things you should do to protect your computer from hackers and viruses. Hackers are always looking for “holes” in the Internet-related software you use. Software companies are constantly discovering weaknesses in their software and making fixes. In a moment, I’ll mention the specific programs you should always check.

But first, it’s most even more important to make sure Windows itself is being updated with the latest security patches and fixes. The good news (again) is that unless you have changed it, Windows Updates are **setup to automatically happen**.

If you’ve ever seen a pop-up message at the lower left side of your screen, saying that “updates are available” or “updates have been done”, Windows is doing the updates for you automatically.

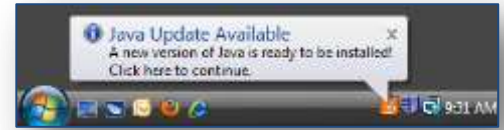
But you can double-check by going to START / CONTROL PANEL / and then choosing **Windows Update**. On the screen that appears, choose CHANGE SETTINGS and you’ll see how Windows Update is currently set.



Patch Tuesday - Starting with Windows 98, Microsoft started allocating the second Tuesday of each month as when they would provide Windows updates. This day has become known as “Patch Tuesday”, and the press often carries news about “how many fixes” Microsoft is sending you that month. Sometimes Microsoft has so many important fixes to do that they add an extra patch Tuesday to the month, 14 days after the first one.

Besides Windows, there are other Internet-related programs you should keep up to date. Although almost all the programs on your computer need updating at one time or another, with many of them it's not really critical that you do the updates.

However, there are a handful of programs that you **SHOULD** allow to update when a notice to do so appears down by your Windows notification area.



- **Adobe Flash** – A special browser plug-in that allows you to see different types of animation and media on the Internet.
- **Adobe Reader** – The program that lets you open, read, and print PDF (portable document format) files.
- **Java** – A program needed for some web sites to properly work, and also for some special programs (such as Open Office) to work on your computer.
NOTE: I suggest you UNINSTALL Java unless you really need it.
- Your favorite **browser** (Google Chrome, Mozilla Firefox, Internet Explorer)

3. Create Strong Passwords – Just about every web site you visit now has options for you to create your own “free account”, which includes creating a “password” to access the account.



Google (www.google.com) is a good example of this.

If you setup a free account with Google, you get access to Gmail, Google Drive (free storage), Google Documents (free word processor and spreadsheet), Picassa (free photo storage), and LOTS more. When you setup a Google Account, you enter your email address (as your username) and **then choose a password**.

You should also make sure that all of your **Internet-related passwords are secure**. This means creating a password that a hacker can't steal or guess.

*Most Hackers use **three basic methods** to guess or steal your account passwords.*

Phishing e-mail – You get an e-mail message that seems to be from a legitimate company (like your bank, or eBay), telling you there is a security problem and asking for you to verify your account information by going to a particular link. You click the link, which takes you to a legitimate looking page, but it's really not. You enter your information, and the hacker has it. Most legitimate companies would **NEVER send a request like this**. You can also tell the site you are going to is fake, but the address.



More on Phishing - Phishing emails have become so common that many Internet users get at least one every day. That's why they are such an important Internet threat to know about. Again, most companies such as banks, eBay, PayPal, and other financial related sites will NEVER send you an email with a link to click inside of it. If you do get an email like this and you're wondering if it's real, close the message, open your browser, and visit the site yourself in the normal way.

Dictionary crack – A hacker uses a program that goes through an entire electronic dictionary, trying all the words in the password field of your account. Not only do they try all the single words, but they often use word combinations and even words spelled backwards.

Brute force – A hacker uses a program that generates random characters and submits them at high speed to a password field.

To see how well-developed the password hacker world is, visit
www.password-crackers.com

So, how do you create a hacker-proof password? Here are some examples of passwords, starting with those that weak.

- **Weak Passwords** – include common words, names, dates, or any other information that can be identified with you. Here are some of the most popular, WEAK passwords that people regularly use (and in fact, this was the top 10 list for 2012 as reported by the web site SplashData (www.splashdata.com)).

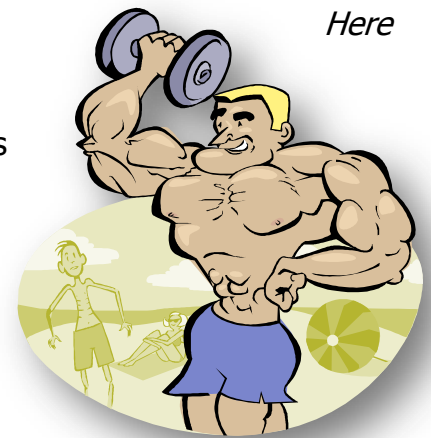
Password	monkey
123456	letmein
12345678	dragon
abc123	111111
querty	baseball

- **Strong Passwords** – The BEST passwords are unique and consist of a long mixture of upper and lower case characters, special characters, and numbers.

For example: **Lc14&68*#@#9f4**

are some tips on creating a strong password:

- ✓ Strong passwords are NOT obvious – don't use dates or names someone can associate with you
- ✓ Don't use any real words found in the dictionary, even spelled backwards!
- ✓ Use both upper and lower case characters
- ✓ Use at least one special character (such as an asterisk *)
- ✓ Make it at least 8 characters long, if not longer
- ✓ Use different passwords for different sites, or create a "regular" and "secure" password to use in different situations



*My best **suggestion for creating a strong password** that you can actually remember is to do this...*

- Think of a favorite song or poem or saying
- Take the first initial from each word
- For each letter that could be a number, change it to that number (for example, "L" could be a "1", "S" could be "5", "O" could be zero, etc.)
- Add your favorite number and capitalized initials to each end.

For example, I could take the phrase "she longs to be close to you" and create this password:

JBL551tbctyJBL5

I don't know about you, but I think that's a pretty darn good password that I might actually be able to remember!

How do I remember all those passwords? If you find yourself with lots of passwords to remember, there are some Web-based and Software-based solutions you can check...

- **LastPass** (www.lastpass.com) – a free web-based password and information manager that actually works with your browser to remember passwords.
- **PasswordSafe** (www.passwordsafe.com) – a free web-based password manager that gives you access to your passwords from any computer.
- **Handy Passwords** (www.handypassword.com) - \$15 – Passwords manager software you install locally.
- **RoboForm** (www.roboform.com) - \$29 – Another local passwords manager program.
-

Remember, too, that **Internet Explorer, Firefox, and Google Chrome** all have features that automatically store Web page username and passwords, and then fill them in for you later.

- ✓ In **Firefox**, go to the menu, then OPTIONS / OPTIONS / Security.
- ✓ In **Internet Explorer** go to Tools / Internet Options / Content/ AutoComplete-Settings button.
- ✓ In **Chrome** go to the menu, then Settings / Show Advanced Settings / Passwords and Forms.

Viruses

A Virus is a small program that has been written specifically to **secretly enter** your computer, **replicate**, and then **spread** to as many files or other computer systems as it can. Once on your computer, they can delete or corrupt important files, replicate until they fill your computer's memory or hard drive, or just act as a nuisance by displaying messages or locking up your computer.



One interesting thing to note is that viruses **rarely completely disable or crash your computer**. "Killing the host" computer would prevent the virus from spreading, so most viruses are written not to crash your computer, but instead to use it for some other deed or just create a nuisance.

Viruses are normally categorized according to how they infect your computer. Here are the most common virus categories you see discussed in the popular press, followed by how they infect and the typical symptoms you see:

Program viruses attach themselves to real programs and then replicate and spread whenever that program is started. Some program viruses have been known to infect just about every other executable (program file) on your computer, so that you are left with hundreds of copies of the virus to somehow get rid of.



Macro viruses (which were especially common in the mid and late 1990's) infect files created by programs that use macro languages, such as Microsoft Word and Excel. In our profession as college instructors, we routinely encountered macro viruses when students turned in homework assignment files on floppy disk or through e-mail.

Worms (which are the most common type of virus today) replicate themselves, and often attempt to spread to other systems through network connections or by E-Mailing themselves to addresses in your E-Mail programs address book.

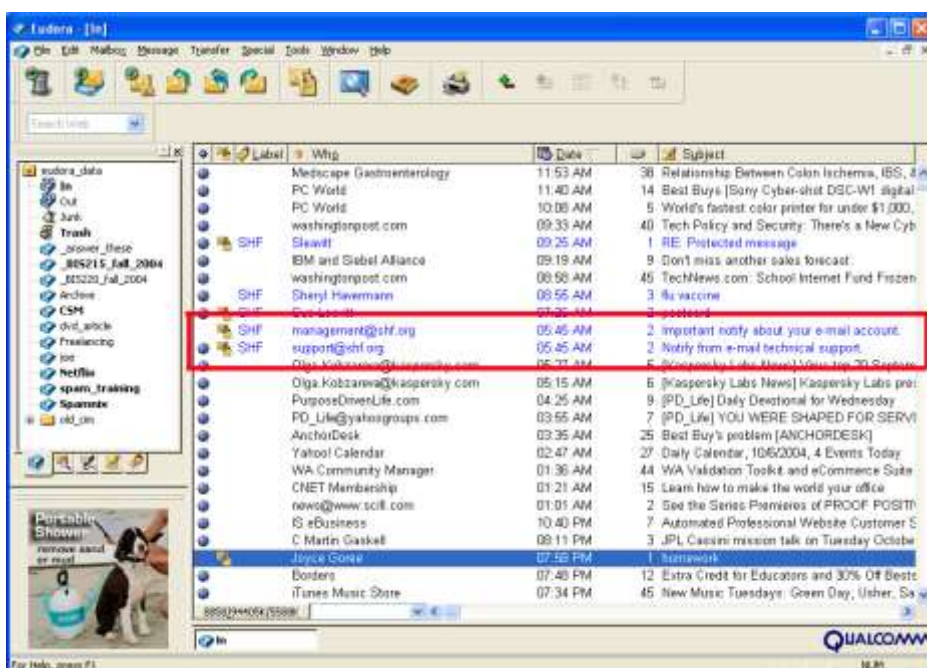


Trojan Horses which we talked about earlier with Hackers, are not really viruses, but small programs that are dropped onto your computer by a virus or hacker attack, automatically start when you re-start your machine, and then open bigger holes in your security so that hackers can take control of your computer, or hide and wait for a particular date and time, and then deliver some type of a “payload” (i.e. they do something you don’t want them to do).



Viruses can **infect your computer in various ways:**

1. They can come in the form of an **E-Mail attachment** (which is a file) that when opened, infects your computer. This is the #1 method of infection. If you get a virus as an e-mail attachment, and do not open the attachment, you are not infected even though the virus is on your computer.



2. They can be attached to **software** that you might download from the Internet. Most popular download sites (which we list in a moment) pre-check the files you download to make sure they have no viruses. It’s the less reputable sites that sometimes can have downloadable software or documents that have viruses attached.
3. They can come on **flash drives and removable drives** from other people.



4. They can come across **local area network connections**, where hard drives have been shared. This is the most common way viruses spread inside of businesses, or even inside of homes that have their computers networked together.



There is a **wide array of symptoms** you might see when infected with a virus, ranging from nothing at all (if the virus is hiding and waiting to go off) to the corruption or deletion of important files. For example, here are some common symptoms you might encounter:

- ✓ Your computer behaves in a way you've never seen before, even after restarting it.
- ✓ Unusual sounds, music, or visual displays that occur at random times
- ✓ Programs start unexpectedly
- ✓ Files suddenly become deleted, damaged, or changed
- ✓ Your computer dramatically begins to slow down as you use it.
- ✓ You begin getting lots of Illegal Operation errors that you can not relate to anything else.

Of course, other things can cause these symptoms as well. A bit later I'll mention a few ideas of what to do if you get infected.

Who Creates Viruses? You've already read about **hackers** and how they often use viruses in their attacks on computers. Other types of computer people that have been known to write viruses include **Script Kiddies** (young teenagers who know just enough about computers to visit hacker web sites and download virus creation programs), **disgruntled employees**, and certainly, **computer terrorists**.

One story goes that after fall of the Berlin Wall, many east-bloc computer engineers found themselves out of work. Disgruntled, they started getting back at the West by hacking and sending viruses their way.

Protecting Yourself Against Viruses

In the old days, you could actually protect your computer from most viruses by just being vigilant. Today, that's almost impossible.



For example, being cautious and only open e-mail attachments from friends and relatives does not protect you from a worm virus that infects a friend's computer, and then automatically sends itself to everyone (including you) in their address book. To make matters worse, new worm viruses will open your e-mail address book, send to everyone in it, and spoof the address by making it appear someone listed in the address book sent the virus.

With that in mind, here are your best methods of protection against a virus infection:

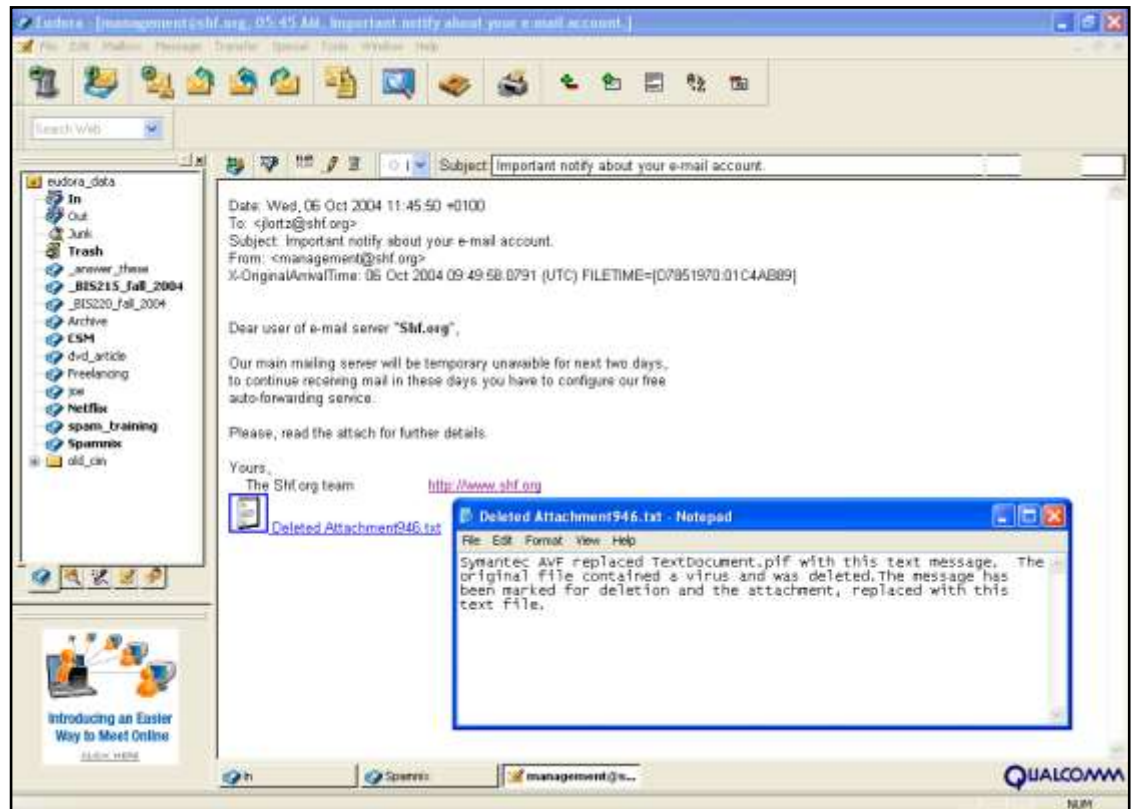
1. Use an Anti-Virus program – Anti-Virus programs constantly monitor your computer, and prevent virus infection by:



- ✓ Checking all **incoming** E-Mail attachments
- ✓ Checking all **outgoing** E-mail attachments
- ✓ Checking all the files you **download and save**
- ✓ Checking programs that start on the **Web pages** you browse
- ✓ Checking **removable media** you insert (floppies, CDs, flash drives, etc.)
- ✓ Periodically **scanning your computer** memory and hard drives
- ✓ **Staying updated** by downloading new virus definitions each day

NOTE OF CAUTION: As I mentioned previously with firewalls, you should only have **ONE** Anti-virus program installed at a time, since they can interfere with each other.

Here is an example of a message that was “disinfected” by an Anti-virus program. Some Anti-virus programs automatically take care of a detected virus, while others will prompt you and give you a choice what to do. In just about all cases, your best choice is to completely delete the virus and the message it was attached to.

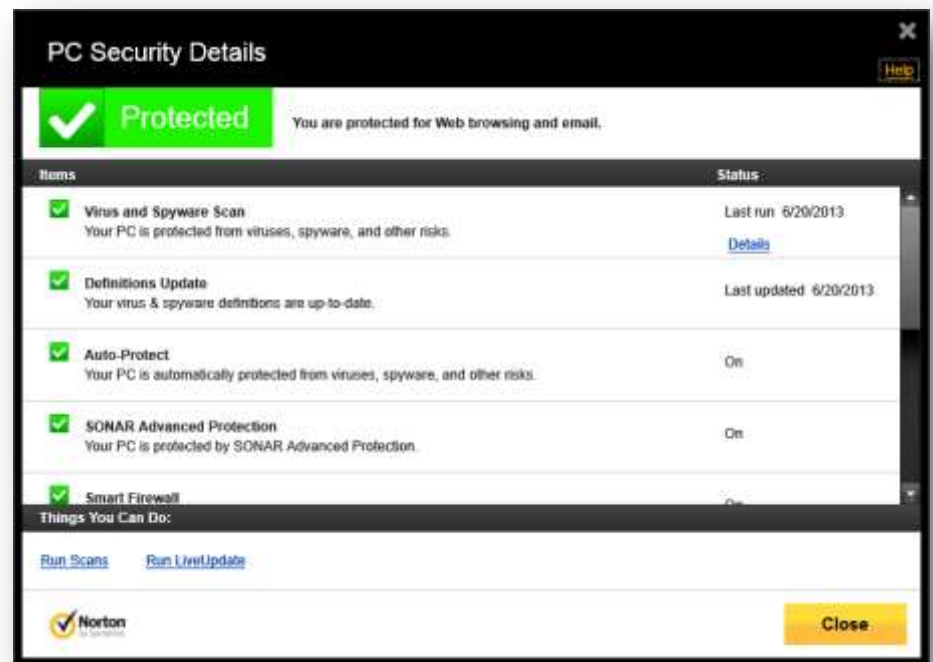


Here are some popular Anti-Virus programs, and where you can get more information and download them. Note that **AVG** and **AVAST** are free, and although they have fewer extra features than the pay-for virus checkers, they are still quality programs that do a good job of protecting you.

- ✓ Norton Internet Security - www.symantec.com
- ✓ Kaspersky Anti-Virus - www.kaspersky.com/
- ✓ AVG Anti-Virus (free) - free.grisoft.com
- ✓ AVAST Anti-Virus (free) - www.avast.com/eng/down_home.html
- ✓ Microsoft Security Essentials (free) - www.microsoft.com/security_essentials/



2. Keep the Anti-Virus program up to date - Each day new viruses are introduced to the world. For your AntiVirus program to work, you must keep the program's **virus definitions** up to date. The company that makes your anti-virus program is constantly adding new viruses to a special virus database that the program uses as it detects virus infections. Most companies provide weekly updates of the definitions.



Modern Anti-Virus programs **automatically** prompt you when to check for updates or new definitions, or just download and install them automatically as you browse the Internet. However, it's still a good idea to routinely open your anti-virus program and check to see if the updates are being done. On the program screen, look for a definition date and make sure it's not more than two weeks old.

3. Let your Browser help you out. - There's always a possibility that a Web site you visit might drop a small script or program on your computer that can do some damage or open up a hole in your security.

You can help prevent this by checking certain browser settings, and making sure they are blocking these types of scripts and other potential dangers.

- ✓ In Internet Explorer, go to **Tools/Internet Options / Security/Custom Level**
 - Under Downloads, Disable **File downloads**
 - ALSO in this section:
 - Disable **unsigned active X controls**
 - Disable any option for **unknown active X controls**
 - Set **Java Permissions** to High safety

Similar browser security settings are found in Google Chrome and Firefox. Here's how to get to those sections...

- ✓ **Google Chrome** – go to Customize button (upper right hand side), choose Settings, then scroll to the bottom of the screen and click Show Advanced Settings. Especially notice the section called Privacy.
- ✓ **Firefox** – go to the Firefox button (upper left side), choose Options and then Options again. In the window that appears, pay particular attention to the Privacy and Security sections (click the top buttons).



4. Be cautious of E-Mail Attachments – Earlier we mentioned that vigilance is not the best method to prevent virus infection. Still, it's a good idea NOT to open an e-mail attachment from someone you don't know. And even with friends, don't open an attachment unless you are expecting it.



If you are wondering whether an attached file is a virus, it's good to know that most viruses are some type of **executable file**, including those with the following file name extensions:

.vbs .exe
.com .scr
.pif

5. Download from reputable sites - Downloading is one of the least common ways to get a virus, unless you visit “**warez**” or pirated software sites. Reputable download sites pre-check your downloads and make sure there are not viruses attached.

By far, my favorite “safe” place to download from is Download.Com, part of CNet.

www.download.com



6. Keep a Backup of Your Important Data - If you do get a virus, you may have to completely wipe your machine and start from scratch, just to get rid of it. When this happens, having a backup of your important data and files is very important.

Wondering how to do a backup? Doing backups requires a bit of knowledge about your files (how things are saved) and folders (where they are saved). This is a complete topic in itself, and in fact, I have a book on the subject entitled **Working with Files & Folders**.

You can learn more about it at www.DiscoverFileOrganization.com.



What if you get a virus?

If your computer becomes infected with a virus, and you have an Anti-virus program, there's a good chance that the virus will disable the anti-virus program, or find a way to hide from it. When this happens, you'll scan your computer and find nothing wrong.

If you think you might be infected, it's a good idea to do the following:

- Go online and visit one of the many sites that provide an **online scanning service**. By scanning your computer for viruses from the Internet, the virus has no chance to disable your scan, and will usually be detected.

Most of the sites that offer this service, have you download a small program (a scanner) and then run that program to do the scan.

3 of our favorite include:

- ✓ **Norton Security Scan** -
securitycheck.symantec.com
- ✓ **Trend Micro Housecall** -
housecall.trendmicro.com/
- ✓ **Panda Cloud Cleaner** -
pandacloudcleaner.pandasecurity.com



- Once you have cleaned your computer of infection, it's a good idea to uninstall, and then reinstall your regular anti-virus program, in case it was damaged by the infecting virus.

If you have your **original anti-virus CD**, you can also use it to help get rid of an infection. Most anti-virus CDs have an "emergency mode" which lets you boot your computer from the CD, and then perform a scan directly from the CD. This can work well for older viruses, however, keep in mind that the virus definition file being used from the CD is out of date, and may not be effective against newer viruses.

As a last resort, you can take your sick computer to your **local repair-person** who will probably do some of the things I just suggested. But as computer geeks, they are a bit more comfortable doing them. Expect to pay from \$50 to \$150 to get your computer disinfected.

Spyware and Malware

The third member in our short list of Internet threats besides Hackers, Phishing Emails, and Viruses is this thing called Spyware. The term **Spyware** is actually a generic term that lumps together a number of different types of malicious or nuisance programs.

These small programs are left on your computer from freeware/shareware programs, media players, and certain interactive Web pages. In recent times, the more malicious spyware programs have been lumped together with viruses, since they can act in a similar way. And in fact, many anti-virus programs also protect you from spyware.

*Spyware can be divided into two general types, **adware** and **malware**.*

Adware

This type of Spyware includes programs that primarily generate **advertisements** on your computer or **tracking your purchasing and browsing habits**. Although most adware programs sneak onto your machine and are unwanted, there are a few shareware and freeware programs that you might use, such as the Weatherbug (www.weatherbug.com) that are considered adware, even though they are very useful.



In this case, you choose to have the program on your computer in return for putting up with the advertisements it displays.

Adware programs are not usually directly harmful, but are **a nuisance that can use up computer resources and slow down your computer**. Some of the things they can do include:

- ✓ Install on your computer without you even knowing it.
- ✓ Generate more pop-up windows than normal, as you browse the Internet.
- ✓ Build a profile of your browsing habits and generate pop-up ads that match what you like to shop or browse for. This type of adware is often called a **dataminer**.

Other terms for adware include **Parasites** and **Scumware**, both of which are referring directly to shareware and freeware you install that simply use up your valuable computer resources (hard drive space, memory, processor time, etc.).

Malware

This is **the most serious type of spyware program**, and is specifically created to invade your computer, hijack Windows and certain application functions, and actively prevent you from removing it.



The only real difference between malware and a virus is that malware makes itself a lot more visible to you through its harmful actions. Viruses tend to hide, multiply, and then attempt to spread, while malware actively causes you problems.

One of the most common ways to get a malware program is by downloading a shareware or freeware program from an unfamiliar site. And of shareware programs, the most notorious for including malware are the **Peer to Peer Clients** (programs often used to share music and video on the Internet).

For example, when you install the popular Internet file sharing program, **Kazaa**, it also includes a program called **Gator**, which is a Trojan that masquerades as a helpful program, but is really spyware that integrates with Windows, tracks which Web pages you visit, and then displays pop-up ads on your desktop. It also tracks the information you type into online forms.

A few software types considered malware include:

- ✓ **Keyloggers** – Record every keystroke you enter (including personal information, account numbers, passwords, etc.) and send them to a hidden Internet address.
- ✓ **Browser hijackers** – Change your browser home page to some undesirable site, and then won't let you change it back.
- ✓ **Toolbar hijackers** – Add what seems to be a useful search toolbar to your browser, when in fact you can't turn the toolbar off or uninstall it. And generally, the toolbar takes you to Web pages that are less than desirable, and tracks your browsing habits.

Where Does Spyware Come From?

The most common place to pickup spyware is **sites that offer free programs, games, funny videos, jokes, and pornography**. These types of sites are big draws, and are typically used by shady marketing companies to drop spybots and adware on your computer. It's also common to see spyware and malware included with freeware and shareware programs you download.

For example, as you browse the Internet, it's not uncommon to suddenly see a **pop-up window** that warns "you might be infected with a virus" or some other nasty thing. It then tells you to **CLICK HERE** to run a special scan and get things fixed.



The truth is, when you click you are taken to a **shady site** that drops something **nasty** on your computer.

FREE is a bad word with Google: One of the most common things folks like to search for is FREE stuff. But be warned! Going to Google and typing in something like "free desktop backgrounds" will bring up some legitimate sites for getting backgrounds, but also some shady sites that might drop some adware or malware on your computer. So just be careful!

How Does Spyware Infect Your Computer?

With regards to HOW they infect you, **Web-based spyware** often infects your computer through what are called **ActiveX controls**, which normally help a Web page provide special types of content, and extend the abilities of your browser. In the wrong hands, ActiveX spyware can infect your machine and cause lots of browser and Windows problems.

Spyware also shows up in the form of **BHO's** (Browser Helper Objects), which are DLL files that add capability to your browser, such as a new toolbar.

Again, in the wrong hands, BHO's can give a spyware program complete control over your browser.

What do you see with Spyware and Malware?

We already mentioned a few of the things you see when infected with Spyware, but here are a few other common symptoms you might run into:

- ✓ A new toolbar suddenly shows up with your browser. (**toolbar hijack**)
- ✓ Your browser homepage changes. (**browser hijack**)
- ✓ Windows or your browser suddenly stop working correctly, and you see more pop-up ads, some of which you can't close.
- ✓ You see more icons in your taskbar notification area (lower right side).
- ✓ New programs load each time you start Windows.
- ✓ In Windows, Web pages are used to display some of the operating system functions. Spyware can infect these pages, and even if you delete the spyware from the system, as soon as you access a control page that's infected, the spyware is re-copied to your computer.
- ✓ You attempt to download, install, or run an anti-spyware program, and the spyware prevents it from happening.
- ✓ You attempt to change your browser settings (Tools pulldown menu, and then Options), and you can't.

Getting Rid of the Problem, and Protecting Yourself

Here's the good news (which I've already mentioned)... Most current Anti-Virus programs also include Anti-Spyware capability, especially for the bad type of spyware we call Malware.

BUT... If you do get infected with spyware or malware programs (and you WILL, even if you do only a small amount of Web browsing), there are a lot of things you can do to get rid of the pests, and protect yourself in the future.

Here are some methods you should try:

- **Use a browser other than Internet Explorer.** Browser related Spyware is usually specific for a particular browser. Since most people use Internet Explorer, most Spyware is written for that browser. To cut down on Spyware, try a popular alternative choice to IE, such as **Mozilla Firefox**, which you can download for free from www.mozilla.com. You might even find you enjoy using it more than Internet Explorer.



You can also go with a browser like **Google Chrome** (chrome.google.com) which is my personal favorite.

Before installing a freeware or shareware program, go to Google and type in the name of the software, followed by the word "spyware", to see if any sites or news sources discuss the program as being spyware.

- The **best way** to rid yourself of spyware and malware programs is by using some of the free and inexpensive anti-spyware programs. I have some listed here...
 - **Adaware** – (www.lavasoft.com) – free program that helps eliminate spybots from your computer. Is also now a great Anti-Virus program!
 - **Spybot S&D** (www.safer-networking.org) – free program that helps eliminate adaware and spybots from your machine, and also lets you clean out your browser cache. As with Adaware, now also includes Anti-virus.
 - **Microsoft Security Essentials** (www.microsoft.com/security) – a program from Microsoft that handles spyware AND viruses.

- **SpywareBlaster** – (www.brightfort.com/spywareblaster.html) a free realtime program that works with Internet Explorer and Mozilla/Firefox to block spyware and adware from invading your machine.
- **SpySweeper** (www.webroot.com) - \$29.95, free 30 day trial. One of the best pay-for anti-spyware programs and is also an anti-virus program.

NOTE: As I've already mentioned, many of the companies that product Antivirus programs like Norton and McAfee, have what they call "Internet Security" solutions, which include not only Anti-Virus capability, but also Anti-Spyware and Firewall solutions. When you purchase one of these programs, be sure to check the box (or web site) to see if their product also includes protection for

Keeping Private Information, Private!

Over the past few years, stories of Internet users losing private information online have become commonplace, leading many to be paranoid about **online shopping** and **online banking**.

Although it's always good to be cautious, as I've been mentioned all the way through this book, the truth is, you can safely shop and bank online, as long as you take a few important precautions and are smart about it.

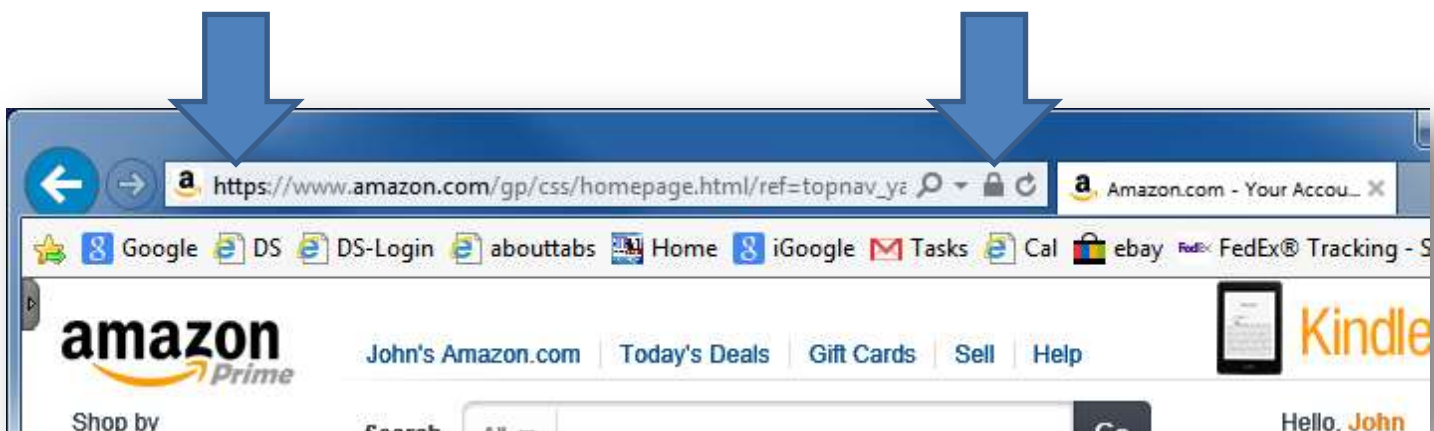
Let's look at some ideas about keeping your private information, private.

Online Transactions and Personal Information

Some of the Web sites you visit, including banks and online stores, require you to type in and submit personal information, such as **credit card numbers**, **account numbers**, **address information**, etc. Normally, when you type your information on the screen, and then click a button to submit it, **the information is NOT encrypted**, and there's the possibility of someone intercepting and stealing it.

To safeguard and encrypt the information you're submitting, you need to make sure you are entering that information on a **secure Web page**. You can tell a Web page is secure by looking for two things on the page:

- ⇒ You should see a small, closed, **padlock** somewhere on the address bar. With many browsers you can click this padlock and get more security information.
- ⇒ The Web page address should start with **https://** rather than **http://**



To make sure your browser is correctly set to handle the encryption that secure pages provide, you should check to see if **SSL** (Secure Sockets Layer) technology is turned on (it normally is). To do this in Internet Explorer do the following:

- Start Internet Explorer, and go to **Tools gear / Internet Options / Advanced /**
- Under Security, make sure Use **SSL 2.0 and 3.0** are checked

SSL Certificates

Now that we've discussed the importance of using secure Web pages when making online transactions, we need to talk a bit more about the technology behind those transactions.



We already mentioned that behind a secure Web page, the technology that makes the security work is called **SSL** (Secure Sockets Layer). SSL uses a private key to encrypt your data before it's sent across the Internet. At the other end, a secure server receives the information. To ensure that you are sending your encrypted data to the server of a legitimate company, that server must have a **digital SSL Certificate** issued or "signed" by a Certificate Authority.

A **Certificate Authority** is a trusted third-party organization or company that issues digital certificates. The CA guarantees that the holder of the digital certificate is who he or she says he or she is. The issuing party typically confirms the information provided to it by credit card verification.

Rather than pay a fee to a Certificate Authority, some online vendors choose to "**self-sign**" their certificates. When your browser encounters a Web page associated with a self-signed Certificate of Authority, **a warning window appears indicating that the certificate was not recognized**. As a user, you have the choice of continuing with the transaction or stopping. If you are sure the company you are working with is legitimate, you can certainly continue the transaction. However, your best choice is to use companies that have gone to the trouble of obtaining a signed certificate from a legitimate Certificate Authority.

Know Your Merchant

Besides entering your information onto a secure page and being aware of SSL Certificates, when you shop online make sure that the merchant site you are visiting is a “known entity”.



What I mean by this is... **know who you are buying from.**

That's easy to do with large stores (such as Target, Wal-Mart, etc.), but what about smaller businesses you've never heard of? There are a couple things you should do...

- Do a Google search on the business name and see if anything negative appears.
- Carefully check the business contact information and make sure they have a working phone number or contact email address.
- Check the site “policies” information to make sure they accept returns, and how they handle complaints or inquiries.

Browser Cookies

Cookies are small files that Web sites send to customers' computers so they can track what a customer has been doing on their site, or to save information about the user so that next time they visit the site, the site knows who they are.



Although **most cookies are harmless** and help make certain Web pages work correctly, cookies can also be used in conjunction with Spybots to track your browsing habits, and generate unwanted pop-up ads.

Here are some cookie facts:

- Some are encrypted and some are not
- Often they are not a security threat, but a **convenience and are necessary**
- In theory, only the site that issues the cookie has permission to see it
- If you disable cookies (which you can do in your browser settings), you may find that many of the sites you visit on a regular basis no longer work the way they did!

What becomes a bit scary about cookies is if various web companies subscribe to the **same web marketing company**, the sites can leave a cookie on your system that tells the Web marketing company when you have visited one of the member sites.

The Web marketing company's cookie can't read other cookies, but it can track how many times you have visited member sites and what pages you visited, building a profile of your online use. Then **targeted banner ads** can be displayed at you.

For example, you might visit PetsOnline.com and check dog collars. And then when you head over to PillowsAreUs.com, the first ad that you see is for dog pillows.



Here's what is inside of a typical cookie from Yahoo:

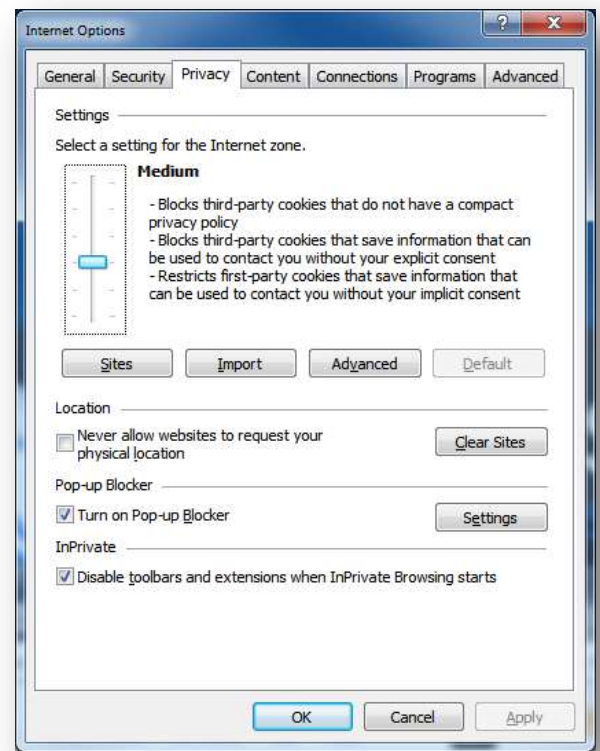
```
B
aarmh5tma2t0a
yahoo.com/
0
985407488
30072022
1599511584
29352471
*
Y
v=1&n=7ejdp&k0f8a7s&l=jme_3e6i_2ec/o&p=m 1p22i42130005&r=4n&lg=us&intl=us
yahoo.com/
0
985407488
30072022
191471136
29390459
```

Anti-spyware and Internet Security programs are very good at eliminating unwanted cookies, and running those programs on a routine basis should take care of most of your “bad” cookie problems.

If you do decide that you no longer want to accept cookies, you can set your browser to prevent them from being saved. **However, you will probably notice that many of the web sites you visit will no longer work!**

To Turn off the cookie feature of your browser.

- In Internet Explorer, go to TOOLS / INTERNET OPTIONS / PRIVACY tab, and adjust the slider to the desired level.



Secure E-Mail

E-Mail is a great way to communicate with others and keep in touch. However, E-Mail is **not typically secure**, since it can be intercepted and read by others (who know how) on the Internet. E-Mail also suffers from the problem of **spam (junkmail)**.



To protect yourself and others, when you use e-mail:

- Don't send sensitive information via e-mail
- If you must send sensitive information, encrypt your message.

- You can download a program called **PGP** (Pretty Good Privacy) which lets you encrypt files before you send them as attachments.
- PGP uses **public key encryption**, where you use a special PGP program to generate a private key, which you then use to generate a public key you exchange with others.
- You can encrypt your own personal files with your own private key, or encrypt them with someone else's public key so they can open the file, if you send it via e-mail or on disc.
- Use a **free Web-based e-mail** account for your **junk mail** or when you are signing up for free services
- **Don't reply to spam**, since it just tells the spammer they have a "live E-Mail" account.
- Don't forward **hoax virus messages** or **chain letters**
- Use the **BCC field** when sending to a group of people, so they don't see each others addresses
- Use **copy and paste** when forwarding a overly forwarded message that includes other peoples addresses in the text
- **Turn off the HTML function** in e-mail, to prevent possible malicious code from doing strange things

Anonymous Browsing

Every time you access a Web page, the site you are contacting can collect certain pieces of information from you, including:

- Your IP address
- Your type of computer, screen resolution, and CPU
- The browser you are using
- Your ISP's name and the Web site you were last on
- If you have one of it's cookies on your computer



And, as we've already mentioned, Web sites can also leave cookies on your machine, and some require that you sign-up (for free) to gain access to their features and information. To protect giving out any information when you browse a site, there are online services that allow you to browse "through them", providing a secure, anonymous browsing experience.

Anonymizer.com (\$79.99/yr) (www.anonymizer.com)

Anonymity 4 Proxy (www.inetprivacy.com/a4proxy)

The-Cloak (www.the-cloak.com)

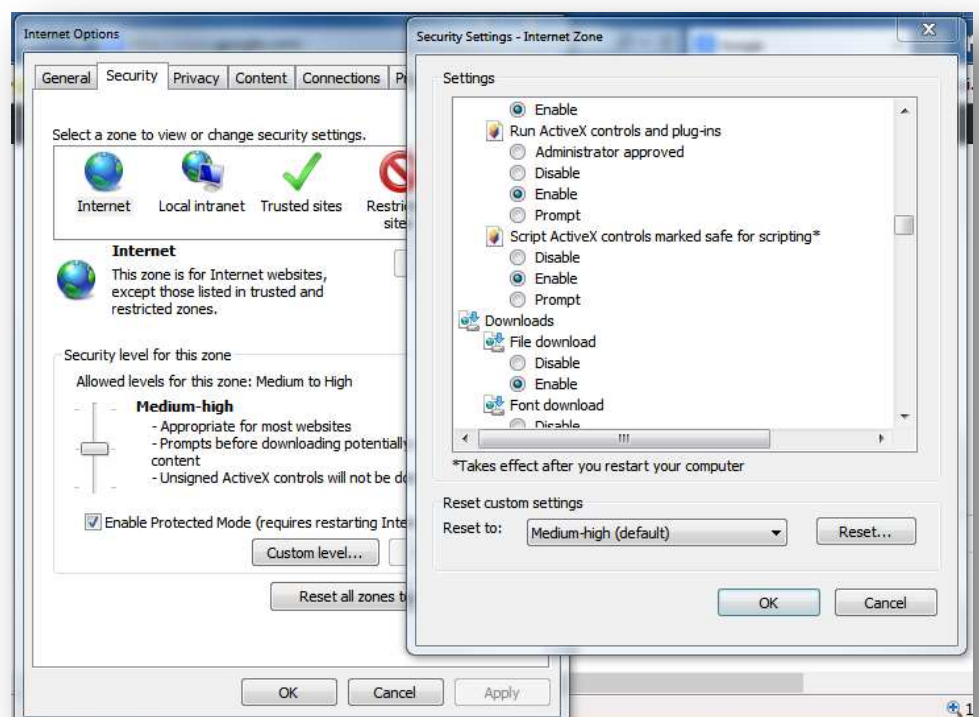
VPN Proxy (www.spaceproxy.com)

ActiveX Controls and Java Applets

To make a Web site more interactive or animated, some Web programmers use **ActiveX Controls** and **Java Applets**. Both are small programs that your browser downloads and then runs to create the interaction.

As you might guess, ActiveX Controls and Java Applets can also contain viruses, spyware, and other malicious code that can cause problems.

You can set your browsers ActiveX and Java security settings by going to Tools / Internet Options, and then the Security Tab. On the tab, click the Internet icon, and then the Custom Level button.



On the list of security items, you'll see a section that deals with ActiveX. Your goal is to disable those ActiveX features you feel you don't need. You will also see a very small section on Java Permissions (or Java VM). Here, you should always set the option to "High Safety".

JAVA SECURITY NOTE: Over the past year, JAVA has had some major security issues that lead me to say you should just uninstall it from your computer unless you absolutely need it. After you uninstall it, if you do encounter a site that needs it you can simply reinstall the latest version from Sun Microsystems, the company that produces Java.

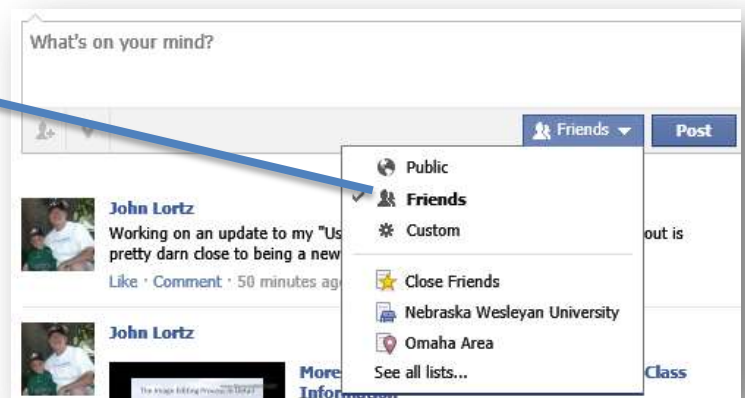
Facebook Privacy



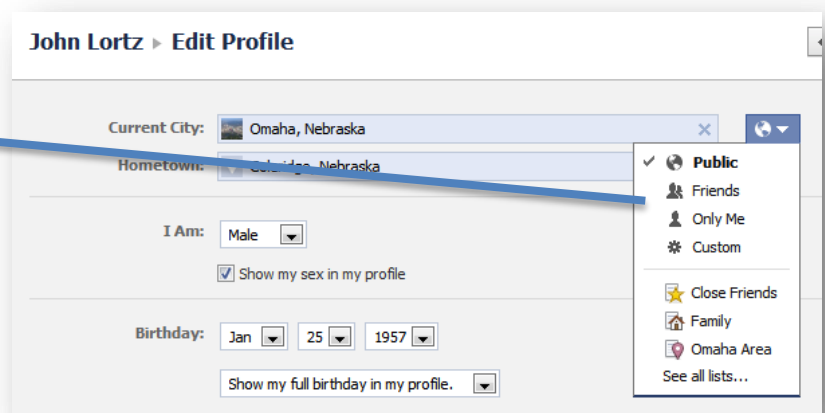
As I end this section on keeping your private information private, I would be amiss not to mention how to keep things private on Facebook.

In a nutshell, you set privacy on Facebook "on the fly" in two places...

- Each time you enter something in the **"What's On Your Mind" box**, you can set WHO will see the post by clicking the drop-down button in the lower right corner.



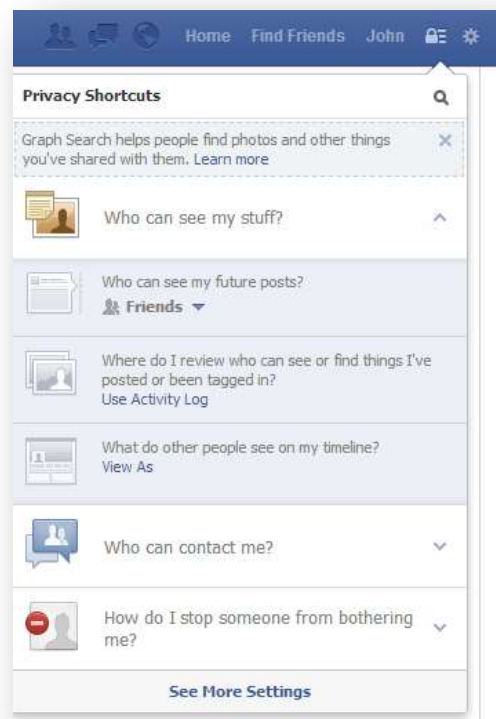
- As you type in your **Profile information**, you can set the Privacy for each individual item.



Besides these two important ways to set Privacy, you can also get to some less important Privacy settings by going to the **drop-down padlock button**, to the right of the Main Menu.

On the menu that appears, you can quickly see and set the privacy for Who Can See My Stuff, Who Can Contact Me, and How Do I Stop Someone from Bothering Me.

You can click the small arrow at the upper right corner of each button to expand the menu and see more choices.



The bottom-line is... for most situations, choosing **FRIENDS** as the option here is your best bet.

Finally, the most important and perhaps easiest way to keep private information private on Facebook is to NOT POST IT in the first place! If there's something personal you don't want the world to know, just don't put it up on Facebook.

Where Do I Go from Here?

Although we've covered a lot of useful ground in this Book, there's always more you can learn. That's both the up, AND downside to something as powerful and useful as the Internet and trying to keep yourself safe as you use it.

Once you've taken the time to put these safety techniques in place, and picked out the ones you personally find the most appealing, you may be satisfied to just continue using these same techniques on a day to day basis.

But if you find yourself wanting to go even FARTHER, we would love to have you as a regular visitor to our learning site, www.DiscoverSkills.com.

On the site you'll find lots of technology articles and videos about technology and how you can use it on a daily basis. The technology I talk about includes LOTS of information about the Internet and keeping safe.

And when you visit the site, you'll see a box where you can subscribe to our FREE eNewsletter, which arrives in your email Inbox about once a week (sometimes twice if we have lots to talk about).

Until then, Have Fun and Stay Safe as you browse and use the net. And be sure to let me know how things are going!



An Internet Safety Checklist

I've covered a lot of geeky topics in this book, so I thought it might be a good idea to summarize all this Internet Safety stuff in a simple summary checklist.

- ☑ Install a good **Anti-Virus program**
- ☑ Make sure your **Firewall** is up and running
- ☑ Make sure your **Windows Updates** are happening
- ☑ Make sure you create **strong passwords** for your online accounts
- ☑ Only enter private information on web pages that are **secure**
- ☑ Never click a **link** in an email that seems to be from a financial institution
- ☑ Only **download** from reputable web sites
- ☑ Always make **backups** of your important files

Appendix A: Resources to Help You to Become More Secure

There are lots of online resources you can access to help you become a more secure Internet user. As we've discussed the threats, we've pointed out some of the sites you should visit. Here are some more you might find helpful.

You can visit these sites to run online tests of your computer security. Most offer a way for you to see how you might be vulnerable, and suggest ways to make your computer more secure (usually by offering you their product).

- Shields up (www.grc.com) (tests the openness of your computer on the net)
- Symantec Security Check – securitycheck.symantec.com
- E-Sof's Security Space – www.securityspace.com
- AuditMyPC - www.auditmypc.com/

You can encrypt sensitive E-Mail messages by using one of the following free online E-Mail services, or by downloading and using the encryption software mentioned here:

- Hushmail.com
- Pop3now.com (online Web access to an existing e-mail account)
- Ziplip.com
- Zixmail.com
- www.pgp.com (must download and install a program)
- Anonymous Remailer (anon.efga.org/Remailers)
- About E-Mail (email.about.com/internet/email/cs/remailers/index.htm)

Other Resources

- www.microsoft.com/security - The Microsoft Security Center
- www.cnet.com/internet-security/ - The CNET Security Center
- www.sans.org – SANS Security Information

Appendix B: A WiFi (Wireless Networking) Primer

Although the focus of this book is Staying Safe, I felt it was important to add this section that discusses wireless networking since it's becoming so common in the home environment, and is the way that many people connect to the Internet.

I'm not going to get into great detail about WiFi here, but just want to give you the basic facts about how it works and what you typically run into when you have WiFi at home.

Wireless technology is part of our lives

Not a day passes that most people don't use some type of wireless connection to communicate or to control something. Examples include cell phones, mobile devices (smartphones), wireless headsets, remote controls, and of course, wireless networking in our homes, and WiFi access in public places.



Wireless Networking and the Frequency Spectrum

Wireless Networking (sometimes called **Wi-Fi**) is really nothing more than **radio signals** being broadcast and received, just like your regular radio or television set.

- With the proper equipment, it's possible to place data (audio, video, bits of information) on the electromagnetic waves that make up a radio signal.
- Your **broadcasting** device and your **receiving** device must be on the same "frequency" (or the same "cycle" as measured in hertz).
- **AM Radio** is broadcast in several frequency bands
 - ⇒ **Long wave** (153KHz to 279KHz) which is not available in the Western Hemisphere because of atmospheric conditions.
 - ⇒ **Medium wave** (530KHz to 1710KHz) which is what we use for AM Radio
 - ⇒ **Short wave** (2300KHz to 26100KHz) which is divided into 15 broadcast bands, and is used by shortwave devices, Police, and CB radio
- **FM Radio** spans from 87.5MHz to 108.0MHz which is part of what we call the VHF spectrum of frequencies (30MHz to 300MHz).

What about Wi-Fi Frequency?

It operates on two separate radio bands

- ⇒ The **802.11b**, **802.11g**, and **802.11n** Wi-Fi standards operate in the 2.4GHz band.
- ⇒ The older **802.11a** standard operates in the 5GHz range, as does the latest (as of this writing) standard called **802.11ac**.
- ⇒ *NOTE: cordless phones share the same bands, which is why they sometimes cause interference with Wi-Fi networks.*

What are the WiFi Standards?

A standard group called IEEE developed a standard for wireless networking called the **802.11** standard in 1997. Since then, newer, faster standards have been developed. Here are the most common standards the home user typically sees:

802.11b – was the first standard that popularized wireless networking. It runs at a 2.4GHz frequency, and transmits at about 11Mbps (which is much slower than a wired network, which is typically transmitting at 100Mbps). Also, the signal is omnidirectional, so you can put a transmitter in a central point and put receives all around it.

802.11a – Operates at 5GHz, and transmits at 54Mbps. It has a directional signal, and so the equipment must be line-of-sight. This standard never became popular because of that.

802.11g – this standard was ratified in June of 2003, and works in the 2.4GHz spectrum, but can operate at 54Mbps. Since 802.11g and 802.11b are totally compatible with each other, this standard became quickly popular.

***NOTE:** Since 802.11b and g both run at 2.4GHz, which is the same as most cordless phones, microwave ovens, and walkie-talkies, there commonly an interference problem. In fact, because of these interference problems, the 802.11g standard often only operates at the level of the 802.11b standard.*

802.11n –this is currently the most popular standard, which builds on the b and g standards by adding MIMO (input/multiple output) and OFDM (orthogonal frequency-division multiplexing). What these two provide is increased data broadcast simultaneously. Runs at both 2.4GHz and 5.0GHz, so has lower interference than b and g. Is backward compatible with other standards.

802.11ac – the latest standard which will probably become more popular over the next few years. It's 3 times faster than 802.11n and even faster than most home wired networks. But since it's new, equipment that supports it is still expensive.

Setting Up a Wireless Network

Your home Internet connection probably looks something like the diagram to the right.

- You pay a monthly fee to an **Internet Provider** (ISP) who runs a cable to your house.
- The cable connects to a **Modem** which in turn is connected to a computer.
- For Wi-Fi, instead of being connected to a computer, the modem is connected to a **Router**.
- The Router sends the Internet signal via **radio waves** out to any device that has a **wireless adapter**.
 - Most desktop computers, laptops, smartphones, and tablets have built-in adapters for Wi-Fi
 - If you have an older computer that does not have an adapter, you can purchase a small **USB adapter** which plugs into your computer, giving it Wi-Fi capability.



- The router signal range is typically **from 200 to 300 feet**, depending upon how your house is constructed and what other radio signal generating devices you might have.

Although the address is a bit long, here is a link to a short CNet How-To video on setting up a wireless network at home.

http://www.cnet.com/4520-7390_1-6213817-

Wireless Security – Public Networks

As convenient as wireless networks are, they also open you up to new **security threats** since you are now communicating with other computers through a radio signal that can easily be picked up by other computers and wireless-ready devices within range of the router.

Before I talk about securing your home wireless network, let me mention something about **using your notebook computer in a public WiFi area** (such as Panera's, McDonalds, a motel, etc.).

Public WiFi networks are just that... **PUBLIC**. This means that when you connect, you are suddenly **connected to anyone else who happens to be using that network**. This also means that if someone had the know-how, they could actually access your computer through the WiFi network, and do just about anything they wanted.

To stay secure in a public WiFi area:

- Have your **Windows Firewall** turned on. This should prevent anyone from hacking onto your computer.

I talked about Firewalls in the earlier section entitled Staying Safe on the Internet.

- **Don't access sensitive sites** or type sensitive information onto a web page when you are connected to a public network. In a public network, you have no control over how the network connection is being established behind the scenes. It would be possible for someone to intercept your unsecure transmissions and hijack whatever they contain. It probably will never happen, but why take a chance.

For this reason, don't access your bank accounts or other sensitive accounts from a public WiFi connection.

Now that we've discussed Public WiFi, let's talk about securing your wireless network at home.



Wireless Security – Your Home Network

To setup your router for Wi-Fi, you must first directly connect a computer to it (using a cable) and use that computer's browser to pull-up a special setup screen that is built-into the router.

One very important part of this setup screen will be the wireless network security.

NOTE: *All routers come with instructions that walk you through setting them up, including properly setting the network security. Be sure to carefully read these instructions.*

Here are the key security options you should look for when you setup your router's security:

- **Change your SSID** – Service Set Identifier (also called BSSID or ESSID) – This is a unique code that identifies your network. Each device you want to connect to the wireless network must be configured to recognize this code to attach to the network. You should ALWAYS change this code from what the manufacturer has set it to, by default.

Make sure you choose a long SSID code. Most let you have up to 32 characters or numbers.

- **Disable SSID broadcasting** – Most routers transmit their name (SSID) publicly every few seconds, which makes it easier for new devices to connect to the Wi-Fi network as they roam.

However, broadcasting the SSID also makes it easier for hackers to discover it which brings them one step closer to hacking your network. **Disabling it in the router** setup means a device has to know the SSID name and have it manually entered the first time you connect.

- **Turn on WEP** (Wired Equivalent Privacy) or **better yet, turn on WPA or WPA2** (Wi-Fi Protected Access) – WEP, WPA, and WPA2 are all standards for encrypting and securing a wireless network. Enabling this on your router means that a device can only connect to it if it has the proper credentials (password/passcode).
- **For even higher security, set up a MAC (Media Access Control) filter** – A MAC address is a 12-digit hexadecimal code that identifies each hardware device of a network. If your network supports MAC address filtering, you can configure your access point to recognize only those devices that have a specified MAC address.

Enable the router Firewall – most wireless routers include firewall capability (NAT – network address translation) and / or true firewall packet inspection.

Disclaimer, Terms of Use, & Trademarks

The author and publisher of this eBook and any accompanying materials have used their best efforts in preparing this eBook. The author and publisher make no representation or warranties with respect to the accuracy, applicability, fitness, or completeness of the contents of this eBook. The information contained in this eBook is strictly for educational purposes. Therefore, if you wish to apply ideas contained in this eBook, you are taking full responsibility for your actions.

The author and publisher disclaim any warranties (express or implied), merchantability, or fitness for any particular purpose. The author and publisher shall in no event be held liable to any party for any direct, indirect, punitive, special, incidental or other consequential damages arising directly or indirectly from any use of the material in this eBook or accompanying materials, which is provided “as is”, and without warranties. As always, the advice of a competent legal, tax, accounting, computer, or other professional should be sought. The author and publisher do not warrant the performance, effectiveness or applicability of any sites or software listed or linked to in this eBook.

All links are for information purposes only and are not warranted for content, accuracy or any other implied or explicit purpose.

All products, sites, and software mentioned are registered trademarks of their respective companies or organizations. They are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this eBook.